IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

LIGHTSPEED MEDIA CORPORATION, Plaintiff, v. ANTHONY SMITH, SBC INTERNET SERVICES, INC., d/b/a AT&T INTERNET SERVICES; AT&T CORPORATE REPRESENTATIVE #1; COMCAST CABLE COMMUNICATIONS, LLC., and COMCAST CORPORATE REPRESENTATIVE #1 Defendants.	Case No. 3:12-cv-889-GPM-SCW Judge: Hon. G. Patrick Murphy Magistrate: Stephen C. Williams

OPPOSITION TO DEFENDANT **ANTHONY SMITH'S** MOTION TO DISMISS AMENDED COMPLAINT

INTRODUCTION

Defendant Anthony Smith's Motion[1] pursuant to Rule 12(b)(6) and L.R. 7.1 fails to identify a single valid ground to dismiss any claim in the Complaint, and the Court should deny it in its entirety. As with the ISPs that have also filed motions to dismiss in this action Smith takes a shot-gun approach seeks dismissal for everything claimed against him. And as with the ISPs, he has failed at every turn to show any ground for dismissal under Rule 12(b)(6). Smith betrays a misunderstanding of the most rudimentary grounds for dismissal under that Rule, asserting that "Smith is innocent of those baseless aspersions" relating to him in the Complaint.

[1] For reference purposes, this memorandum refers to Defendant Anthony Smith as "Smith," the Federal Rules of Civil Procedure as "Rules;" the Local Rules of the U.S. District Court for the Southern District of Illinois as "L.R.;" the Amended Complaint as "Complaint" or "Compl." and citations thereto as ECF 2-2; the Rule 12(b)(6) motion to dismiss as "Motion;" its supporting memorandum as "Supporting Memo" or Supp. Mem.;" Plaintiff, Lightspeed Media Corporation as "Lightspeed;" Internet Service Provider as "ISP;" and the Federal Computer Fraud and Abuse Act as "CFAA."

(Supp. Mem. at 1.) The time for Smith to challenge the accuracy of the allegations, of course, is at trial. It is not a proper basis to seek dismissal. Smith's legal arguments are also baseless. Stripped of its voluminous string-citations to inapplicable case law and incorrect or irrelevant factual assertions (which, again, are impermissible basis upon which to seek dismissal under Rule 12(b)(6)), Smith's arguments reduce to the following: that Plaintiff has not alleged "loss" and "damage" under the CFAA; that the claims are pre-empted by the Federal Copyright Act; and that the Plaintiff has not alleged the required elements of the claims arising under Illinois law. The Court should deny the Motion and order Smith to promptly answer the Complaint.

Plaintiff notes at the outset that Smith seeks to incorporate by reference arguments made by the party ISPs in their motions to dismiss. (*See, e.g.,* Supp. Mem. at 7.) His reasons for doing so are because his Motion already duplicates several of the failed arguments that the ISPs already made. To the extent the Court allows those memoranda to be "incorporated into" Smith's Motion, Plaintiff incorporates by references its responses in opposition to them (ECF No. 39, 40) as well. Furthermore, Smith's Supporting Memorandum is peppered with augments appearing in footnotes. There are twenty-two such footnotes in his Supporting Memorandum. Whether Smith's intention is to artificially fit his Supporting memorandum within the required page limit, this practice is not acceptable in courts within the Seventh Circuit. Indeed, it is clear that a party waives arguments that appear only in a footnote. *See Bakalis v. Golembeski*, 35 F.3d 318, 326 n. 8 (7th Cir.1994) (holding that an argument is waived if it was made only footnote and not fully developed in an opening brief). The Court should disregard notes 1 through 22.

BRIEF FACTUAL BACKGROUND

Even the most inattentive review of the Complaint clearly demonstrates that this is not a copyright action. Smith chooses to ignore that fact and premises his Motion on arguments that,

even if they were correct (which they are not), would be properly argued in an action involving claims for copyright infringement. Smith could have avoided needlessly wasting the Court's time if he had based his arguments on what is actually in the Complaint, rather than what he may have been charged with if he were in a copyright case action.

Smith needn't have bothered making the vast majority of the arguments in his motion, because this is not a copyright case. This case is about computer hacking and theft, Plaintiff alleges that Smith is the primary hacker and thief. Smith is alleged to be the "master hacker" who illegally broke into Plaintiff's websites with hacked passwords, took protected content, and assisted others who participated in the same "hacking community" as he to do the same.

As set forth in the Complaint, Plaintiff is the owner and operator of adult entertainment websites. ECF 2-2 at ¶16. Plaintiff invests significant capital in maintaining and operating those websites. *Id.* Plaintiff makes the websites available only to those individuals who have been granted access to Plaintiff's website content (*i.e.,* paying members). *Id.* This access is given to members of the Plaintiff's websites who sign-up and pay a fee to access the content. *Id.* Access to this content is protected by a password assigned to each individual member.

Smith, as the Complaint alleges, along with many co-conspirators formed a hacking community, where hacked passwords are passed back and forth among the members. ECF 2-2 at ¶17. Members in this community work together to ensure that the members have access to normally inaccessible and unauthorized areas of Plaintiff's secured websites. *Id.* The series of transactions in this case involved accessing, agreeing to share, and sharing hacked passwords over the Internet and using the hacked passwords to access Plaintiff's protected websites and private computer content. *Id.* Defendant Smith and his co-conspirators actively participated

with one another in order to disseminate the hacked passwords, and intentionally engaged in a concerted action with one another to access the same websites and content. *Id.*

Defendant Smith and his co-conspirators gained unauthorized access to Plaintiff's protected websites. ECF 2-2 at ¶18. They used hacked passwords to intentionally gain unauthorized access to the member's sections of Plaintiff's protected websites. *Id.* Through these hacked passwords, Defendant Smith and his co-conspirators consumed Plaintiff's content as though they were paying members. *Id.* They downloaded Plaintiff's private computer content and disseminated that information to other unauthorized individuals. *Id.*

Since Defendant Smith and his co-conspirators accessed Plaintiff's protected websites through hacked passwords, they were not required to provide any identifying personal information, such as their true names, addresses, telephone numbers or email addresses. Defendant and his co-conspirators can only be identified by their IP addresses. ECF 2-2 at ¶19.

Plaintiff retained Arcadia Data Security Consultants, LLC ("Arcadia") to identify IP addresses associated with hackers that use hacked passwords and the Internet to access Plaintiff's protected websites and private computer content. ECF 2-2 at ¶20. Arcadia used forensic software named Trader Hacker and Intruder Evidence Finder 2.0 (T.H.I.E.F.) to identify hacking, unauthorized access, and password sharing activity on Plaintiff's websites. ECF 2-2 at ¶21. The individuals committing these unlawful activities are identified by their IP addresses as well as the dates and times they unlawfully accessed Plaintiff's websites. *Id.*

Once Defendant Smith and his co-conspirators' IP addresses and dates and times of unlawful access were ascertained, Arcadia used publicly available reverse-lookup databases on the Internet to determine what ISP issued the IP addresses. ECF 2-2 at ¶22. In addition to logging Defendant Smith's IP address, Arcadia's software logged other important information

into a uniform database, such as the specific websites that were unlawfully accessed and the files that were downloaded during that unauthorized access. ECF 2-2 at ¶23.

Defendant Smith was detected by the T.H.I.E.F. Security System gaining unauthorized access to Plaintiff's protected websites on November 24, 2011 at 01:09 (UTC). ECF 2-2 at ¶24. This date was the latest time the T.H.I.E.F. Security System detected Defendant's unauthorized access. Defendant was detected by the T.H.I.E.F. Security System accessing, without authorization, ten (10) of the Plaintiff's protected websites. Further, Defendant was detected downloading more than seventy-two (72) private computer files from these websites. ECF 2-2 at ¶25.

Plaintiff attached a listing of the IP address, ISP, and date and time of one of unauthorized accesses of Defendant Smith and his co-conspirators as an Exhibit to the original Complaint. A declaration attesting to Arcadia's software is attached as an Exhibit to the original Complaint, a signed copy of which is on file with the Court in this matter. ECF 2-2 at ¶26.

Smith, along with the other members of his hacking community, and their respective ISPs, thus enabled and sheltered the continued massive hacking into and theft from Plaintiff's website. The extent of the hacking is demonstrated by the fact that between August 1 and December 6, 2011 alone, Plaintiff's software blocked well over 330,000 unauthorized sign-on attempts to its website (over 2,500 per day). ECF 2-2 at ¶50. The IP addresses listed in the Complaint represent less than two percent (2%) of the attempts to hack into Plaintiff's website. *Id.* at ¶51. In total, hackers illegally downloaded over 170,000 files, using more than 3.5 terbytes of total bandwith, from Plaintiff's website. *Id.* Furthermore, upon information and belief, nearly twenty percent, or 1,805, of the group of subscribers that the ISPs seek to protect have attempted to hack into Plaintiff's website with a new, hacked user passcode, since this litigation began. *Id.*

at ¶52. This amount continues to increase daily. Of those, at least seventy-five have each attempted to hack Plaintiff's website five or more times each since this action began. *Id.*

ARGUMENT

A Federal litigant must plead sufficient factual matter that, if accepted as true, will state a claim to relief that is plausible on its face. *See Ashcroft v. Iqbal,* 556 U.S. 662 (1949) (2009); *Twombly,* 550 U.S. 544 555 (2007). The plaintiff must plead "factual content [that] allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal,* (1949). The standard governing a Rule 12(b)(6) motion incorporates two important and related principal. First, the complaint cannot rest upon conclusory assertions, or simply allege legal conclusions portrayed as facts. *See Kendall*, 518 F.3d at 1048. *Twombly* and the cases following it require that a complaint allege "not just ultimate facts (such as a conspiracy), but *evidentiary facts* which if true, will prove" the alleged violation. *Id*. at 1047 (quoting *Twombly*, 550 U.S. at 555) (emphasis added); *see also Iqbal*, (courts are "not bound to accept as true a legal conclusion couched as a factual allegation") (internal citation omitted); *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001) (court need not accept "merely conclusory, unwarranted deductions of fact").

Under Rule 12(b)(6), "dismissal for failure to state a claim is proper only if it is clear that no relief could be granted under any set of facts could be proved consistent with the allegations." *Cervantes v. City of San Diego*, 5 F.3d 1273, 1274 (9th Cir. 1993). This rule challenges the sufficiency of a pleading, and it must be read in conjunction with Rule 8(a) which provides the standard for a well-plead complaint in Federal Courts. 5A Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* §1355-56 (1990) ("[A] short and plain statement of the claim showing that the pleader is entitled to relief."). Furthermore, a court "must accept all

material allegations in the complaint as true, and construe them in light most favorable to the plaintiff." *NL Industries v. Kaplan*, 792 F.2d 896 (9th Cir. 1986). Accordingly, the court's task in a Motion to Dismiss adjudication is a limited one; "[t]he issue is not whether plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims." *Vega v. JP Morgan Chase Bank, NA*, 654 F. Supp. 2d 1104 (E.D. Ca. 2009) (quoting *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974)). As such, dismissal under a Rule 12(b)(6) motion is only proper 'where there is either a "lack of cognizable legal theory" or "the absence of sufficient facts alleged under a cognizable legal theory." *Id.* (quoting *Balistreri v. Pacifica Police Dept.*, 901 F.2d 696, 699 (9th Cir. 1990)).

Smith's attempt to avoid liability through a baseless proclamation of his innocence is irrelevant and improper under Rule 12(b)(6), and the Court should ignore such statements in the Motion. Defendant's arguments that the claims are pre-empted by the Federal Copyright Act fail because there is no claim for copyright infringement. Smith's claims that Plaintiff has not alleged the required elements of its various claims fails legally, because Plaintiff plead all necessary allegations for each count. The Court should therefore deny the Motion. Plaintiff's Complaint easily satisfies this standard for each count.

I. PLAINTIFF HAS ALLEGED A CLAIM UNDER THE FEDERAL COMPUTER FRAUD AND ABUSE ACT IN COUNT I

Smith's argument that Plaintiff has not alleged claims under the CFAA is based upon the premise that Plaintiff has not asserted enough facts to allege "loss" or "damages" under the CFAA. (Supp. Mem. at 5-8.) That premise is incorrect; Plaintiff has alleged a substantial number of facts to allege that it incurred both damages loss under the CFAA.

In Count I, Plaintiff alleges that Defendant Smith violated the CFAA by, among other things, using a hacked username/password to gain access to Plaintiff's site, and purposefully

disseminating content to unauthorized individuals. The CFAA, among other things, provides a right of action in such circumstances. Specifically, the CFAA at Section 1030(a) lists actions subject to liability, including intentionally accessing a computer without authorization; obtaining information from, a protected computer without authorization; causes transmission of a program or information from a computer; traffics in passwords used to access a computer without authorization. *See* 18 U.S.C. § 1030(a). Plaintiff has alleged that Defendant Smith engaged in all of that conduct, and Smith's claim that he cannot ascertain which parts of the CFAA that he has violated ring hollow and do not justify dismissal.

Furthermore, the FAA imposes liability for any person who "*conspires* to commit … an offense" under Section 1030(a) is liable for civil penalties. 18 U.S.C. § 1030(b) (emphasis added). Plaintiff alleged at the outset of the Complaint that it is against both Defendant Smith, and his co-conspirators. ECF 2-2 at ¶1. Plaintiff brought the action against Smith and his co-conspirators for, among other things, civil conspiracy and violation of the CFAA and alleged that he and others repeatedly and persistently hacked into and steal from Plaintiff's website. ECF 2-2 at ¶2[2].

As such, Plaintiff has properly alleged both that (1) Smith directly hacked into Plaintiff's website, and (2) Smith conspired with other hackers to hack into and steal from those sites. Smith's argument that the Complaint lacks allegations to impose liability under CFAA Section 1030 is thus demonstrably false. Plaintiff's allegations, when viewed in the light most favorable to Plaintiff as the Court must in response to a Rule 12(b)(6) motion, properly allege that Smith is directly liable for damages under CFAA Section 1030(a), and that he is liable for conspiring with his co-conspirators under the CFAA Section 1030(b).

---

[2] Count I (and every other Count in the Complaint) incorporates by reference all allegations preceding it in the Complaint. Compl. at ¶53.

Plaintiff sufficiently alleged that it incurred loss and damage in accordance with the CFAA. Courts in the Seventh Circuit have held that either loss *or* damage must be alleged in order to state a claim under the Act: "Thus, to recoup compensatory damages, a plaintiff must show *either* damage or loss." *Farmers Ins. Exchange v. Auto Club Group,* 823 F.Supp.2d 847 (N.D. Ill. 2011) (citation omitted); quoting *US Gypsum Co. v. Lafarge N. Am. Inc.,*670 F.Supp.2d 737, 743 (N.D.Ill.2009). "Thus, to recoup compensatory damages, a plaintiff must show *either* damage or loss." *Farmers Ins. Exchange v. Auto Club Group,* 823 F.Supp.2d 847 (N.D. Ill. 2011) (citation omitted); quoting *US Gypsum Co. v. Lafarge N. Am. Inc.,*670 F.Supp.2d 737, 743 (N.D.Ill.2009). "In short, a person suing under section 1030(g) must prove: (1) damage *or* loss …" *Motorola, Inc. v. Lemko Corporation,* 609 F.Supp.2d 760 (N.D. Ill. 2009); "To state a civil claim for a violation of the CFAA, the plaintiff must allege `1) damage or loss; 2) 998*998 caused by; 3) a violation of one of the substantive provisions set forth in § 1030(a); and 4) conduct involving one of the factors in § 1030(c)(4)(A)(i)(I)-(V).'" .*Customguide v. Careerbuilder, LLC,* 813 F.Supp.2d 990, 998-99 (N.D. Ill. 2011) (citing *Cassetica Software, Inc. v. Computer Scis. Corp.,* No. 09 C 0003, 2009 WL 1703015, at *3 (N.D.Ill. June 18, 2009).)

a. **Plaintiff Sufficiently Alleged "Loss"**

Plaintiff has sufficiently alleged that it has suffered a "loss" as defined in the Act, which defines that term 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." 18 U.S.C. § 1030(e)(11). Plaintiff alleged that "The cost to Plaintiff … to identify Defendant and other hackers was in excess of $250,000." ECF 2-2 at ¶57. The allegations in Plaintiff's Complaint sufficiently allege

that it has suffered a "loss." As Chief Judge Holderman held in *Farmers Insurance Exchange v. Auto Club Group,* "Loss" also pertains to "any revenue, loss incurred, or other consequential damages incurred" by the defendant. *Farmers,* 823 F.Supp.2d at 854, *citing* 18 U.S.C. §1030(e)(11). A plaintiff asserting a claim under the Act can satisfy its obligation to plead loss by "alleging costs reasonably incurred in responding to an alleged [Act] offense, *even if the alleged offense ultimately is found to have caused no damage as defined by the [Act.]* *Id.* (emphasis added). In *Farmers,* the Court agreed with another decision in the U.S. District Court for the Northern District of Illinois holding that a plaintiff adequately plead loss under Act Section 1030 by alleging costs of at least $5,000 in terms of responding to the defendant's conduct the plaintiff's damage assessments. *Id.;* citing *Sam's Wine and Liquor, Inc. v. Harting,* No. 08 C 570, 2008 WL 4394962 at *4 (N.D. Ill. Sept. 24, 2008).

Plaintiff alleged that, as a result of the actions of Defendants' acts or omissions, it had to take remedial actions in order to prevent the rampant and ongoing unauthorized access to its protected websites and private computer content. ECF 2-2 at ¶57. Plaintiff further alleged that its cost for Arcadia to create the T.H.I.E.F. Security System to identify Defendant and other hackers was in excess of $250,000. *Id.* It alleged that the cost to host and run that System is $500 per month and that its total cost to host and use the system was $5,500. *Id.* at ¶58. Plaintiff alleged that the average subscription to its website lasts 2 months; that Smith and other conspiracy members have damaged Plaintiff in the amount of $519,350 in lost revenues by gaining, or allowing and failing to prevent, unauthorized access to Plaintiff's protected websites instead of authorized access; and that Defendants have caused harm to Plaintiff in the amount of at least $774,850 in economic damages for the remedial measures Plaintiff was forced to take to

prevent further unauthorized access to its websites by Defendant Smith and other hackers. *Id.* at 59-60.

Defendant bases his entire loss argument on the fact that Plaintiff has not pled an "interruption of service." As an initial matter, there is no such pleading requirement. The plain language of 18 U.S.C. § 1030(e)(11) shows that the subsection contains two independent clauses. The first clause is: "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information prior to the offense." The second clause is: "any revenue lost, cost incurred, or other consequential damages incurred because of interruption in service." The two clauses are separated by the conjunction "and." Due to the presence of a conjunctive, in plain English the phrase "interruption in service" only modifies the second clause, as Chief Judge Holderman has ruled. *Farmers,* 823 F.Supp.2d at 854. Further, Plaintiff *did* plead an interruption of service. The operative service in question is Plaintiff's authentication computer service, upon which the integrity of its entire business rests. Plaintiff pled that the Defendant hacked into Plaintiff's authentication service and disabled it by distributing hacked passwords to thousands of his co-conspirators, rending the authentication service inoperative.

b. Plaintiff Sufficiently Alleged "Damage"

Defendant also argues that Plaintiff did not plead "damage." With respect to damage Defendant claims that the damages alleged by Plaintiff do not relate to any "impairment to the integrity or availability of data, a program, a system or information." ECF No. 37 at 6. Defendant's conclusion is plainly wrong. In its FAC, Plaintiff alleged impairment of its entire computer program that authenticates users. Plaintiff alleges that Defendant hacked into Plaintiff's website, generated false passwords and then distributed the false passwords to his hacking community. ECF 2-2 at ¶17. This process impaired the computer program that

authenticates users (an impairment that continues to this day) because the ubiquity of these hacked passwords fatally impairs Plaintiff's authentication software from distinguishing legitimate users from illegal users.

II. THERE IS NO FEDERAL PREEMPTION OF ANY OF PLAINTIFF'S CLAIMS DUE TO THE FEDERAL COPYRIGHT ACT

Smith's argument regarding preemption is fatally defective. To put his argument in its proper context, take the example of a member's only web-based service: Westlaw. According to Smith, such a service could never assert a state law claim against hackers who hack the authentication scheme and distribute hacked passwords to the public. According to Smith, any such claim would invariably be preempted by the Copyright Act, even though there are substantial categories of private computer content that are not subject to the Copyright Act (e.g. search results and content not copyrighted by Thompson-West.) This conclusion is obviously absurd.

A. Plaintiff Alleged Theft Of Private Files, Not Subject To The Copyright Act.

Smith argues that all of Plaintiff's State law claims are preempted by the Copyright Act, 17 U.S.C. §§ 101, *et seq.* (the "Copyright Act") because "allegations of `unauthorized access" … do not differ *in kind* from the elements of infringement." (Supp. Mem. at 9, emphasis in original.) He further argues that "the additional elements of knowledge and intent do not render [an] asserted right different in kind than the rights protected in a copyright infringement claim." (*Id.,* citations omitted.)

Plaintiff does not, however, seek to recover for the theft of copyrighted material in this action. Indeed, Plaintiff does not allege that its materials are subject to copyright protection; Smith's claim that "One video file and four photographs are the only specific content [Plaintiff] alleges were wrongfully downloaded" (Supp. Mem. at 8) is incorrect and does not appear in the

Complaint. The Court's review is limited to allegations that actually appear in the Complaint in response to a motion to dismiss, and not merely Smith's false characterization of the property that was stolen. Plaintiff alleged that, through hacking, Defendants "gained unauthorized access to data such as identifying exploitable flaws in database codes." *Id.* Plaintiff further that the Defendants "work[ed] together to ensure that the members have access to normally *inaccessible and unauthorized areas of Plaintiff's secured websites*." *Id.* at ¶17 (emphasis added). Plaintiff alleged that "[t]he series of transactions in this case involved accessing, agreeing to share, sharing hacked passwords over the Internet and using the hacked passwords to access Plaintiff's protected websites and *private computer content.*" (*Id.;* emphasis added.) And it alleged that Defendant Smith and his co-conspirators "downloaded private computer content and disseminated that information to other unauthorized users" (*id.* at ¶18) and that Defendant Smith "download[ed] more than seventy-two (72) *private computer files* from [its] websites." *Id.* at ¶25. The phrase "private computer files" incorporates such files as password lists and other user generated information that could not colorably be described as subject to the Copyright Act.

B. Each Claim Involves Pleading Of Elements Not Required For A Copyright Act Claim.

Smith's argument also fails because each claim in the Complaint involves pleading of elements not required for a Copyright Act claim. In each of the six counts alleged against Smith, Plaintiff seeks to allocate liability for the harm that suffered. Each claim relates to whether Smith, acting alone or with his co-conspirators, should be held to be civilly liable for Plaintiff's harm, and not whether they committed copyright infringement of Plaintiff's works. None alleges the existence of copyrightable information, and each is distinct from a copyright infringement claim. Plaintiff does not assert that Smith infringed on its copyright. To the contrary, Plaintiff

claims that Smith is liable for the damage he caused by virtue of its acts and omissions. The harm caused by Smith's acts and omissions are *sui generis* harms distinct from infringement.

The Federal Copyright Act preempts claims arising under state law if they are equivalent to copyright infringement claims. *See* 17 U.S.C. § 301(a); *Higher Gear Health Group, Inc.*, 223 F.Supp.2d 953, 956 (N.D. Ill. 2001). Section 301(a) "`preempts all legal and equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106' [of the Copyright Act] and are in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103." *Seng-Tiong Ho v. Taflove*, No. 10-2144, 2011 WL 2175878, at *8 (7th Cir. Jun. 6, 2011) (quoting 17 U.S.C. § 301(a)). The Seventh Circuit has identified two elements of copyright preemption under Section 301: "First, the work in which the right is asserted must be fixed in tangible form and come within the subject matter of copyright as specified in § 102. Second, the right must be equivalent to any of the rights specified in § 106." *Id.;* quoting *Baltimore Orioles, Inc. v. Major League Baseball Players Ass'n.,* 805 F.2d 663, 674 (7th Cir. 1986). Those rights include the "`reproduction, adaptation, publication, p0erformance and display' of the copyrighted work." *Id.* (quoting *Tomey v. L'Oreal USA, Inc.,* 406 F.3d 905, 909 (7th Cir. 2005)). In order to avoid preemption, a state law claim "must regulate conduct that is qualitatively distinguishable from that governed by federal copyright law – i.e., conduct other than reproduction, adaptation, publication, performance and display." *Id.* (quoting *Toney,* 406 F.3d at 910.)

In this action, there is no allegation of copyright infringement. Plaintiff alleges that Defendants acted to hack into its websites, and steal private information it. There is no allegation that the information included publicly-available information subject to the Copyright Act. At this stage of the proceedings, the Court must accept those allegations as true. *Cole v.*

Milwaukee Area Tech Coll. Dist., 634 F.3d 901, 903 (7th Cir. 2011). The only allegations regarding any copyright come from Smith, which seeks to read them into the Complaint solely for purposes of liability. And each claim against Smith includes an extra element not required for copyright infringement:

III. PLAINTIFF HAS PROPERLY ALLEGED CONVERSION IN COUNT II.

Defendant seeks dismissal of the Count II claim for conversion because it is preempted by the Copyright Act, and because it does not involve the theft of tangible property. (Supp. Mem. at 13-15.) Plaintiff has already addressed Defendant's first argument, and the second is incorrect and fails as a matter of law.

The elements of conversion in Illinois that a plaintiff must allege are that (1) it has a right to property; (2) it has an absolute and unconditional right to possession of the property; (3) it made a demand for possession; and (4) defendant wrongfully and without authorization assumed control, dominion, or ownership over the property. *Cirrincione v. Johnson,* 184 Ill. 2d 10703 N.E.2d 67, 70 (1998). Plaintiff properly alleged each element in its complaint. ECF 2-2 at ¶¶62-67. Defendant argues that he cannot be liable for conversion because the private information he took from Plaintiff was not in a "tangible form." This argument fails. Notably, Defendant devotes some of its argument to whether conversion can extend to intangible *rights*. (*See* Supp. Mem. at 14.) As set forth above, Plaintiff is not seeking to enforce intangible rights relating to its private content. It is seeking to recover damages for the action by Defendant Smith and others into its websites. Furthermore, Illinois law does not, as Defendant argues, preclude a claim for the theft of something that is intangible. As Defendant admits, a cause of action may lie for "personal property which is tangible, or at least represented by *or connected with something tangible.*" (Supp. Mem. at 13, citing *In re Thebus,* 108 Ill.2d 255, 260 (1985). The

private information that Plaintiff alleged Defendant converted was connected with something tangible: Plaintiff's websites. And the private information that Defendant took from it became "tangible" the instance Defendant converted it into a form that he could share with others. Defendant's argument that Plaintiff's private information was "intangible" simply because it was taken from a hacked website is baseless and unsupported in Illinois law.

Furthermore, Illinois law does allow a claim for conversion of Plaintiff's private information because an action for conversion may arise for any chattel that can be described, identified or segregated, and an obligation to treat it in a specific manner is established. *In re Thebus*, 108 Ill.2d 255, 260 (1985)); Illinois Jurisprudence, Personal Injury and Torts § 10:12. Information such as Plaintiff's subscriber information, account records, invoices and other private information that Defendants took from it clearly meet that standard. Furthermore, a claim for conversion is appropriate relating to material such as commercial paper, other valuable papers, or evidence of title to checks, bills, books of account and other documents evidencing title to property. *(Film and Tape Works, Inc. v. Junetwenty Films, Inc.*, 368 Ill.App.3d 462, (1st Dist. 2006)). Plaintiff's claims for the removal of private information, which includes information such as private financial information, that Plaintiff had an obligation to treat it in a specific manner, is clearly appropriate for a claim for conversion. Plaintiff's claim for conversion is thus quantitatively different than, for example, the claim at issue in *Joe Hand Promotions, Inc. v. Lynch,* 822 F.Supp. 2d 803, 808 (N.D.Ill. 2001), which Defendant also relies upon, and which concluded that the tort of conversion does not extend "to intangible property like television programming." Plaintiff does not seek to protect such intangible property.

The case that Defendant relies upon, *In Re Thebus*, to support of the proposition that Defendant's property should not be considered property for the purpose of a conversion claim

because it is not tangible property (Supp. Mem. at 13) was decided before the rise and subsequent mass popularity of the Internet. In *Bilut v. Northwestern*, the Appellate Court of this state found that the plaintiff's research in that case was a proper subject of conversion because the printed copy of the research constituted tangible property. *Bilut v. Northwestern University),* 692 NE 2d 1327 (1998.) What if the research had been on a hard drive, or in a "cloud" storage server? The purpose of the tort of conversion, as cited by Defendant, has been to provide a cause of action for an identifiable object of property of which Plaintiff was wrongfully deprived. Plaintiff thus argues that the purpose of the tort of conversion would be best suited by allowing such actions for identifiable, though intangible, objects of property. The scope of identifiable property today is quite different from that which existed when *Thebus* was decided. Many individuals now find that some of their most valuable possessions exist solely in an electronic format. To limit the grounds for conversion to tangible property, and bar claims on the basis of identifiable property that lies in an electronic medium, would be a failure to interpret conversion within the societal context in which it is alleged. Plaintiff was no less wrongfully deprived of his right to possession of his property merely by virtue of the fact that his property existed in an electronic medium.

IV. PLAINTIFF HAS PROPERLY ALLEGED UNUUST ENRICHMENT IN COUNT III.

Smith's argument that Plaintiff has not sufficiently pled unjust enrichment in Count III fails. Supp. Mem. at 15-16.

In order to allege such a claim, the plaintiff must allege facts suggesting that the defendant has unjustly retained a benefit to the plaintiff's detriment, and that defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience. *See, e.g., Raintree Homes, Inc. v. Vill. Of Long Grove, 209 Ill.2d 408,* 807 N.E.2d

439, 445 (2004). "The doctrine of unjust enrichment underlies a number of legal and equitable actions and remedies." *Martis v. Grinnell Mut. Reinsurance Co.,* 388 Ill. App. 3d 1017, 905 N.E.2d 920 (2009). To establish an unjust enrichment claim under Illinois common law, a plaintiff must show that (1) the defendant has "unjustly retained a benefit to the plaintiff's detriment," and (2) the defendant's "retention of the benefit violates the fundamental principles of justice, equity, and good conscience." *HPI Health Care Servs., Inc. v. Mt. Vernon Hosp., Inc.,* 131 Ill.2d 145, 160, 545 N.E.2d 672 (1989). "For a cause of action based on a theory of unjust enrichment to exist, there must be an independent basis that establishes a duty on the part of the defendant to act and the defendant must have failed to abide by that duty." *Martis,* 388 Ill. App. 3d at 1025, 905 N.E.2d 920. It "is not a separate cause of action that, standing alone, would justify an action for recovery." *Mulliban v. QVC, Inc.,* 382 Ill. App. 3d 620, 631, 888 N.E.2d 1190 (2008). "Rather, it is a condition that may be brought about by unlawful or improper conduct as defined by law, such as fraud, duress, or undue influence, and may be redressed by a cause of action based upon that improper conduct." *Martis,* 388 I*Ll. App. 3d at 1024-25, 905 N.E.2d 920.

Plaintiff has pled unjust enrichment as a separate count. However, that count incorporates a vast number of allegations that Smith unjustly retained a benefit to the Plaintiff's detriment, and that Defendant's retention of the benefit violates the fundamental principles of justice, equity, and good conscience. Plaintiff's claim is properly supported by the conduct of Smith and participating in and allowing others to participate in "unlawful or improper conduct," and it states an appropriate claim for relief in connection with this litigation. Furthermore, Defendant's selective reading of the Complaint to suggest that Plaintiff's only claim for damages is compensation denied to it (Supp. Mem. at 16) disregards numerous other damages that

Plaintiff has suffered, and continues to suffer, as set forth in the Complaint. That argument fails to justify dismissal of Count III.

V. PLAINTIFF HAS PROPERLY ALLEGED BREACH OF CONTRACT IN COUNT V.

Defendant's claim Plaintiff's breach of contract claim does not allege facts sufficient to indicate the terms of the contract and does not allege that a valid and enforceable contract existed (Supp. Mem. at 16-18) also fails.

Plaintiff's Complaint indicates the terms of the contract where it states "to lawfully access Plaintiff's website, users must state that they agree with the following statement: 'I have come to this website knowing it's [sic] contents and agree to view sexually explicit material for my personal use. Viewing such material does not knowingly violate the community standards of the area in which I live.' In return for this attestation, Plaintiff allows individuals to access its website and content." (ECF 2-2 at ¶ 42). Though Defendant accessed the website without authorization, he did access the websites, and though he used a username/hacked password, he was still required to agree to the above-cited attestation in order to access the website. Plaintiff allowed Defendant to access its website and content after receiving this agreement from Defendant, though Defendant did so under the false pretense that Defendant was in fact a paying customer, and not using a username/hacked password to access the site. Taking Plaintiff's factual allegations as true—as they must be in a motion to dismiss—Defendant could be found liable for breach of contract. Defendant is thus not entitled to a dismissal of Count V.

VI. PLAINTIFF HAS PROPERLY ALLEGED CONSPIRACY IN COUNTS VI AND VII.

Smith's argument in favor of dismissing the civil conspiracy claims against him in Counts VI and VII is that Plaintiff has not named all of Smith's co-conspirators as defendants. (Supp. Mem. at 18-20.) This argument fails for two reasons. First, Smith has not cited an

Illinois case holding that a conspiracy must allege claims against all members of a conspiracy. There is utterly no basis in his Motion to support such a far-reaching proposition. And second, as should be obvious to a person with a scintilla of the facts in this proceeding, Plaintiff cannot name all of the co-conspirators in this action because the ISPs have withheld their identities from Plaintiff, and because this Court may not have personal jurisdiction over them when they are identified.

Defendant has not pointed to a single Illinois decision suggesting that he should be dismissed because the more than 6,000 co-conspirators of his are not named as defendants. IT cites only a 2000 unreported California District Court decision and a 1984 Colorado District Court decision. (Supp. Mem. at 19.) To date, however, it has been impossible, despite nearly a full year of active litigation, for Plaintiff to learn the identities of all of Plaintiff's co-conspirators. For those names that it has learned, Plaintiff has actively pursued litigation against the individuals in separate actions and in courts having personal jurisdiction. It is, of course, not possible for Plaintiff to name as co-defendants those individuals whose identities it cannot ascertain. More importantly, there is simply no requirement in Illinois law that Plaintiff must name each of Smith's co-conspirators as a defendant in this action in order to avoid dismissal.

CONCLUSION

For all of the foregoing reasons, Plaintiff respectfully requests that this Court deny the Motion in its entirety, and grant it any and all further relief that this Court deems to be reasonable and appropriate under the circumstances.

[intentionally left blank]

Respectfully submitted,

LIGHTSPEED MEDIA CORPORATION

DATED: October 22, 2012

By: /s/ Paul Duffy

Paul Duffy (Bar No. 6210496)
Prenda Law Inc.
161 N. Clark St., Suite 3200
Chicago, IL 60601
Telephone: (312) 880-9160
Facsimile: (312) 893-5677
E-mail: paduffy@wefightpiracy.com
Attorney for Plaintiff

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on October 22, 2012, all counsel of record who are deemed to have consented to electronic service are being served a true and correct copy of the foregoing document using the Court's CM/ECF system.

/s/ Paul Duffy
PAUL DUFFY