

**IN THE CIRCUIT COURT OF THE TWENTIETH JUDICIAL CIRCUIT  
ST. CLAIR COUNTY, ILLINOIS  
LAW DIVISION**

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

---

Case No. 12-cv-889-GPM-SCW

Judge: Hon. G. Patrick Murphy

Magistrate: Stephen C. Williams

**OPPOSITION TO DEFENDANT COMCAST CABLE COMMUNICATIONS LLC’S  
MOTION TO DISMISS AMENDED COMPLAINT**

**INTRODUCTION**

The Motion<sup>1</sup> by Comcast and its Representative 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. (ECF No. 28.) While Comcast takes a shot-gun approach and seeks dismissal for everything claimed against it and/or its Representative, each of Counts I, IV, VII, VIII and X is well-pled. The arguments that Comcast makes in its Motion include astonishingly incorrect statements of governing law, particularly Federal laws governing cable

---

<sup>1</sup> For reference purposes, this memorandum refers to Comcast Cable Communications, LLC as “Comcast;” the Comcast Corporate Representative #1 as “Representative;” 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 Rule 12(b)(6) motion to dismiss as “Motion;” Plaintiff, Lightspeed Media Corporation as “Lightspeed;” Lightspeed’s amended complaint as “Complaint;” and Internet Service Provider as “ISP.”

communications companies, that Comcast – one of the largest cable providers – should know are incorrect. The Court should deny the Motion in its entirety.

### **FACTUAL BACKGROUND**

Neither Defendant Comcast nor Defendant AT&T Internet Services (“AT&T”) have ever contested or disputed allegations that certain of its subscribers have hacked into, and stolen from, Plaintiff’s website. (ECF No. 2-2 ¶¶ 27-28.) At the outset of this litigation, the ISPs and their Representatives were simply third-party custodians who were the sole holders of identifying information of their subscribers who have been hacking into and stealing from Plaintiff’s website. (*Id.* ¶ 29.) Plaintiff attempted, through the only means available to it, to obtain that identifying information through discovery. (*Id.*)

The Defendant ISPs, upon information and belief, through the approval and authorization of the Corporate Representative of each entity, chose to interpose themselves in this litigation, interfere with the Court’s orders, evade subpoenas, and prevent and obstruct Plaintiff from learning the identities of those ISP subscribers hacking into and stealing from its website. (*Id.* ¶ 30.) Further, upon information and belief, the Defendant ISPs have not taken any actions to prevent their subscribers from committing criminal and tortious acts against Plaintiff even after being on actual notice of the criminal and tortious activity and having full control over the Internet accounts of their subscribers. (*Id.*)

An overwhelming percentage of the alleged criminal and tortious actors are Comcast and AT&T subscribers. (*Id.* ¶ 31.) As such, the delay tactics and other interference on the part of the ISPs have prevented Plaintiff from learning the identities of a vast number of Defendant Smith’s co-conspirators. (*Id.*) Plaintiff requested, and this Court granted (on or about December 16, 2011) leave to serve discovery in order to learn the identities of Defendant Smith and his co-

conspirators. (*Id.* ¶ 32.) In accordance with that Court Order, Plaintiff served subpoenas upon all of the ISPs listed in Paragraph A of the Court Order, including Defendants AT&T and Comcast. (*Id.* ¶ 33.)

Upon being served with the subpoenas, the Defendant ISPs sought to delay and derail this litigation, thereby shielding their subscribers from liability and allowing them to continue their unfettered hacking and theft from Plaintiff's websites. (*Id.* ¶ 34.) The Defendant ISPs ran interference for their paying customers, despite allegations that certain of those customers were using their subscriptions to commit criminal acts. (*Id.* ¶ 35.) The ISPs have not provided the identity of hackers who are also their subscribers to Plaintiff. (*Id.* ¶ 36.) The ISPs instead filed several motions to extend the time in which to respond to the subpoenas. (*Id.* ¶ 37.) The ISPs, rather than responding, moved to quash the subpoenas. (*Id.* ¶ 38.) The Court, after hearing extensive evidence and argument from the ISPs, entered orders on April 27 and May 21, 2012, in which it directed the ISPs, among other things, to produce subscriber information for the Court to review *in camera* before disclosing it to Plaintiff. (*Id.*)

Rather than comply with that order, the ISPs caused further delay by filing a petition with the Illinois Supreme Court under Supreme Court Rule 383, seeking a supervisory order to preclude the disclosure of subscriber information to the Court for *in camera* review. (*Id.* ¶ 39.) The Illinois Supreme Court on June 24, 2012 granted that petition and vacated the May 24, 2012 order. (*Id.*) In seeking to quash the subpoenas, and in submitting the Rule 383 Petition, the ISPs made numerous arguments for which they had no standing, on behalf of its subscribers who have been identified as hackers. (*Id.* ¶ 40.) The ISPs, among other things, challenged on grounds only available to parties to litigation, such as lack of personal jurisdiction, improper joinder,

challenges to the sufficiency of factual allegations in the Complaint under 735 ILCS 5/2-615, and other arguments that are available only to litigants to make. (*Id.* ¶ 41.)

The ISPs also argued that the burden on their subscribers of producing identifying information in response to subpoenas served upon them was excessive. (*Id.* ¶ 42.) The ISPs made this argument despite the fact that the subpoenas imposed no burden on the subscribers because the ISPs, and not subscribers, were the only ones required to take action. (*Id.*) The ISPs chose to act as if they were parties to this litigation, and have obstructed any attempt by Plaintiff to stop the hacking into, and theft from, its website. (*Id.* ¶ 43.) Every action that the ISPs have taken in connection with this litigation has served to delay litigation and to prevent Plaintiff from preventing hacking. (*Id.* ¶ 44.) Every action that the ISPs have taken in connection with this litigation has prevented Plaintiff from asserting its rights, preventing criminal activity against it, or obtaining any relief for harm caused to it. (*Id.*)

The ISPs did not and have not produced evidence suggesting that they have notified any of their subscribers to cease and desist the illegal hacking into, and theft from, Plaintiff's website. (*Id.* ¶ 45.) The ISPs did not and have not produced evidence suggesting that they have cancelled a single contract with a subscriber on the ground that Plaintiff has identified it as having stolen from its website. (*Id.* ¶ 46.) The ISPs did not and have not produced evidence suggesting that they have notified law enforcement officials that certain of their subscribers have engaged in criminal activity against Plaintiff. (*Id.* ¶ 47.) Upon information and belief, the ISPs have taken no reasonable action to prevent the massive level of hacking into, and theft from, Plaintiff's website, which continues to this day. (*Id.* ¶ 48.)

The ISPs and their respective Corporate Representatives have thus enabled and sheltered the continued massive hacking into and theft from Plaintiff's website. (*Id.* ¶ 49.) The extent of

the hacking that the ISPs continue to enable 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). (*Id.* ¶ 50.) The IP addresses listed in the Complaint represent less than two percent (2%) of the attempts to hack into Plaintiff's website. (*Id.* ¶ 51.) In total, hackers illegally downloaded over 170,000 files, using more than 3.5 terbytes of total bandwidth, 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-or passcode, since this litigation began. (*Id.* ¶ 52.) This amount continues to increase daily. (*Id.*) 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, 129 S.Ct. 1937 (2009); *Bell Atlantic Corp. v. 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*, 129 S.Ct. at 1949. The standard governing a Rule 12(b)(6) motion incorporates two important and related principals. First, the complaint cannot rest upon conclusory assertions, or simply allege legal conclusions portrayed as facts. *See Kendall v. Visa USA, Inc.*, 518 F.3d 1042, 1048 (9th Cir. 2008). *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*, 129 S.Ct. at 1950 (courts are "not

bound to accept as true a legal conclusion couched as a factual allegation”) (internal citation omitted); *Sprowell 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)). Plaintiff’s Complaint easily satisfies this standard for each count.

**I. THERE IS NO FEDERAL PREEMPTION OF ANY OF PLAINTIFF’S CLAIMS DUE TO THE FEDERAL COPYRIGHT ACT OR THE FEDERAL COMMUNICATIONS DECENCY ACT.**

Comcast argues at two points that Plaintiff’s claims are barred by federal laws. Perhaps reflecting Comcast’s belief in their relative strength, its *second* argument (rather than its first) is

that all of Plaintiff's claims against it are barred by the Federal Copyright Act. (ECF No. 28-1 at 8-10.) And one of its last arguments is that Plaintiff's conspiracy and aiding and abetting claims are barred by the Cable Decency Act. (ECF No. 28-1 at 14-15.) Comcast's arguments are frivolous for several reasons, not least of which is that, of course, federal law cannot preempted by other federal laws.

**A. Federal Laws Cannot be Preempted by Federal Laws**

Comcast asks this court to be the first federal court in the history of the United States to rule that a federal statute is preempted by another federal statute. The complaint was filed under a federal statute—namely, the Computer Fraud and Abuse Act—and a federal statute (or state law derivate claims) cannot be preempted by another federal statute. Just as the world is not flat, so too cannot a federal statute be preempted by another. Comcast's argument in this regard is, at best, an attempted bon mot.

**B. No Preemption Under The Federal Copyright Act.**

Defendant argues that Plaintiff's claims are preempted because they relate to the theft of files subject potentially subject to Federal copyright protection. (ECF No. 28-1 at 8.) That argument is incorrect on two levels. First, Plaintiff alleged that Defendants stole, or conspired to steal, *private* computer files, not specifically files generally available to the general public upon the payment of a fee. Second, each claim in the Complaint requires establishment of an element not required to establish copyright infringement, and each claim survives under the "extra element" test for preemption under Federal copyright law. Plaintiff has not alleged any copyright violation.

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

Comcast argues that all of Plaintiff's claim for negligence is preempted by the Copyright Act, 17 U.S.C. §§ 101, *et seq.* (the "Copyright Act") because the Complaint "at its core asserts only interests protected by the" Copyright Act "and must be dismissed as preempted..." (ECF No. 28-1 at 8.) Comcast also argues that "at bottom," Plaintiff seeks protection provided under the Copyright Act. (*Id.* at 10.) But the Court must review all of the allegations in the Complaint in response to a motion to dismiss, and not merely what Comcast deems to be at its "core" or "at bottom." And Plaintiff does not allege copyright infringement. Plaintiff instead has alleged that Defendant Jones, and his coconspirators including Comcast, caused or allowed unauthorized access to Plaintiff's website through the use of hacked passwords. (ECF No. 2-2 ¶14.) 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.)

Comcast seeks to use the trick of eliding the phrases "inaccessible and unauthorized areas of Plaintiff's secured websites," and access to "private computer content," to mean information



available to the public for a fee and potentially subject to protection under the Copyright Act. (ECF No. 28-1 at 8-10.) But that is not what Plaintiff has alleged; the Court must evaluate the claims as Plaintiff drafted them, and it is clear that Plaintiff is alleging the theft of private computer content, not information generally available to the public upon payment of a fee. (ECF No. 2-2 ¶¶ 54, 55, 57.) It alleged that Defendants were engaged in the theft of private computer content and private computer files from Plaintiff's websites. It does not allege that they merely stole information that was readily available to the public upon the payment of a fee.

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

Comcast'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 five counts alleged against Comcast and/or its Representative, Plaintiff seeks to allocate liability for the harm that suffered. The claims relate to whether Comcast and its Representative 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 Comcast infringed on its copyright. To the contrary, Plaintiff claims that Comcast is liable for the damage he caused by virtue of its acts and omissions. The harm caused by Comcast'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 (7<sup>th</sup> 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 (7<sup>th</sup> Cir. 1986)). Those rights include the “‘reproduction, adaptation, publication, performance and display’ of the copyrighted work.” *Id.* (quoting *Toney v. L’Oreal USA, Inc.*, 406 F.3d 905, 909 (7<sup>th</sup> 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 (7<sup>th</sup> Cir. 2011). The only allegations regarding any copyright come from Comcast, which seeks to read them into the Complaint solely for purposes of liability. And each claim against Comcast includes an extra element not required for copyright infringement:

The elements of copyright infringement are (i) ownership of a valid copyright, and (ii) copying of constituent elements of work that are original. *See, e.g., Feist Publications, Inc. v. Rural Tel. Serv., Co.*, 499 U.S. 340, 361 (1991). Each claim asserted against Comcast involves

an element substantively and quantitatively different than required for establishment of copyright infringement.

*Count I* alleges a Computer Fraud and Abuse Act violation, for which Plaintiff was required to allege (1) damage or loss; (2) caused by; (3) a violation of the substantive provisions set forth at [18 U.S.C.] § 1030(c) (4)(A)(1)-(V).” *Cassetica Software, Inc. v. Computer Scis. Corp.*, No. 09 C 0003, 2009 WL 1703015 at \*3 (N.D.Ill. June 18 2009). Aside from the nonsensical conclusion that Comcast’s argument, if accepted, would hold that one Federal law preempts another, none of those “substantive provisions” are an element of liability under the Copyright Act, and therefore there is no preemption. Likewise, each of Counts IV, VII, VIII and X, as set forth below, do not involve copyright claims, and include pleading of extra elements not required for a copyright claim. None are preempted.

**B. No Preemption Under The Federal Communications Decency Act.**

Comcast’s second preemption argument, that Plaintiff’s claims for civil conspiracy and aiding and abetting (Counts VII and X, respectively) are preempted by Section 230 of the Communications Decency Act (“CDA,” 47 U.S.C. §230) (ECF No. 28-1 at 14-15), should be stricken under Fed. R. Civ. P. 11.

Section 230 prohibits “hold[ing] interactive computer services liable for their failure to edit, withhold or restrict access to offensive material disseminated through their medium.” Section 230; *see Blumenthal v. Drudge*, 992 F.Supp. 44, 49 (D.D.C. 1998). That provision generally pertains to the content of communications, and Defendant does not cite to, nor is Plaintiff’s counsel aware of, any case where a network operator successfully invoked section 230 immunity for torts arising from the dissemination of non-offensive material. There is a simple reason why such a case does not exist: the CDA relates exclusively to offensive speech.

The CDA was enacted to “deter and punish trafficking in obscenity, stalking, and harassment by means of computer.” 47 USC § 230(b)(5). Congress recognized that holding online service providers (*e.g.*, Facebook or Myspace) and ISPs liable for the offensive speech of their users would foster a “[C]hilling effect upon Internet free speech....” *Zeran v. America Online, Inc.*, 129 F.3d 327, 330-331 (4th Cir. 1998). Such companies would have no option but to deploy aggressive speech filters if they were exposed to tort liability for the offensive speech of their users.

Initially, Comcast’s Section 230 claim is, if anything, an affirmative defense and is not a proper basis for dismissal under Rule 12(b)(2). *Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003) (“What [the ISPs] sought, and what the district court granted, is dismissal under Fed.R.Civ.P. 12(b)(6) for failure to state a claim on which relief may be granted ... Affirmative defenses do not justify dismissal under Rule 12(b)(6); litigants need not try to plead around defenses.”) Furthermore, the cases that Comcast cites relate to tort immunity for offensive speech. (ECF No. 28-1 at 15.) For example, *Doe v. GTE Corp.*, 347 F.3d 655, 655-66 (7<sup>th</sup> Cir. 2003) related to the dissemination of videos of players secretly recorded in locker rooms and then disseminated. *Noah v. AOL Time Warner, Inc.*, 261 F.Supp.2d 532, 532-33 (E.D. Va. 2003) was a suit against an ISP provider “for damages and injunctive relief, claiming that the ISP wrongfully refused to prevent participants in an online chat room from posting or submitting harassing comments that blasphemed and defamed plaintiff’s Islamic religion and his co-religionists.” *Gaston v. Facebook, Inc.* Case No. 12-cv-00063, 2012 WL 62968 at \*1-3 (D. Or. Feb. 2, 2012) involved allegations including defamation, sabotage, attempted murder, and invasion of privacy. *Cornelius v. Deluca*, Case No. 09-cv-00072, 2009 WL 2568044 related to claims of libel. And

*Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193 (N.D. Cal. Jul. 30, 2009), involved allegations that the plaintiff clicked on advertisements that led her to fraudulent websites.

In each instance, the speech in question was identified in the CDA's policy statements. See 47 U.S.C. § 230(b)(5) (ensuring vigorous enforcement of laws designed to, "deter and punish trafficking in obscenity, stalking and harassment by means of computer.") In this case, Plaintiff is not seeking to impose liability on Comcast for its "failure to edit, withhold or restrict access to offensive material disseminated through his residential network." *Blumenthal*, 992 F.Supp. at 49. Instead, Plaintiff is seeking to impose liability on Comcast for allowing, and preventing Plaintiff from stopping, hacking into and theft from Plaintiff's websites. There is simply no basis on which to confer section 230 immunity on Defendant.

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

Comcast argues that Plaintiff does not assert "that Comcast took any action directly affecting protecting computers, or causing transmission of any password ..." in its claim in Count I under the Federal Computer Fraud and Abuse Act ("CFAA," 18 U.S.C. § 1030, *et seq.*). (ECF No. 28-1 4.) That is incorrect, and Comcast's arguments that Plaintiff has not properly pled losses due to Defendant's conduct fails.

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. (ECF No. 2-2 ¶¶ 53-61.) The CFAA, among other things, provides a right of actions in such circumstances. Specifically, the CFAA at Section 1030(a) states 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; or traffics in passwords used to access a computer without authorization. *See* 18 U.S.C. § 1030(a).

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 No. 2-2 ¶ 1.) Plaintiff brought the action against Comcast and its Representative for, among other things, civil conspiracy and violation of the CFAA and alleged that it, directly and through its Representative, allowed Comcast subscribers to “repeatedly and persistently hack into and steal from Plaintiff’s website;” “failed to take reasonable action to prevent their subscribers from hacking into and stealing from Plaintiff’s website; failed to warn their subscribers to cease and desist in such conduct; interfered with Plaintiff’s efforts to identify and take action to prevent the subscribers’ illegal and tortious activity; and **through direct policy decisions**, inaction or for other reasons, allowed the continued and pervasive criminal and tortious acts by certain of [its] subscribers against Plaintiff.” (ECF No. 2-2 ¶ 2) (emphasis added)<sup>2</sup>.

Furthermore, Plaintiff alleged that Comcast and its Representatives “knowingly assisted, or negligently allowed”, the theft from Plaintiff’s website, and that it has “opposed and interfered with Plaintiff’s attempts” to learn the identities of the hackers.” (ECF No. 202 ¶ 3.) Plaintiff that Comcast conspired with Defendant Smith and his co-conspirators by, among other things, failing and refusing to take any action to prevent” the Defendant and others from hacking into, and stealing from, Plaintiff’s websites. (ECF No. 2-2 ¶¶ 27, 56, 57.) Plaintiff’s allegations are

---

<sup>2</sup> Count I (and every other Count in the Complaint) incorporates by reference all allegations preceding it in the Complaint. (ECF No. 2-2 ¶ 53.)

that Comcast and its Representative acted in concert with Defendant Smith and other hackers to hack into and steal from Plaintiff's website.

As such, Plaintiff has properly alleged both that (1) Comcast and its Representative acted in concert with Defendant Smith and other hackers in allowing them to hack into Plaintiff's website, and (2) conspired with Defendant Smith and other hackers to hack into and steal from those sites. Comcast's arguments that the Complaint lacks allegations to impose liability under CFAA Section 1030 are, 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 Comcast is directly liable for damages under CFAA Section 1030(a), and that it is liable as a co-conspirator with Defendant Smith and others under the CFAA Section 1030(b).

Defendant's second argument, that Plaintiff must plead that it suffered "both damage *and* loss in order to properly allege" a CFAA violation and "overcome a motion to dismiss" (ECF No. 28-1 at 6-7), misstates both the CFAA and applicable case law. Comcast relies largely on an opinion from U.S. District Court for the Northern District of Illinois that, at the time, held that a plaintiff had to allege both loss and damages. (*Id.* at 6) (citing *Garelli Wong & Associates, Inc. v. Nichols*, 551 F.Supp.2d 704, 708 (N.D. Ill. 2008)). But Comcast neglects to point out that Congress amended the Act in September 2008, several months after *Garelli* was decided. Among other things, the CFAA no longer includes a Section 1030(a)(5)(A)(iii), which the *Garelli* court relied upon to conclude that a claimant must allege both damage *and* loss. And the CFAA specifically allows for a private right of action for any person who suffers damage *or* loss from a violation: "Any person who suffers damage *or* loss by reason of a violation" of CFAA Section

1030 “may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. § 1030(g) (emphasis added).

Since the Act was amended in 2008, 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)).

Furthermore, 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) (emphasis added). Plaintiff alleged that “The cost to Plaintiff ... to identify



Defendant and other hackers was in excess of \$250,000.” (ECF No. 2-2 ¶ 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 therefore satisfy its obligation to plead damages 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 has met the pleading requirements for alleging a violation of the CFAA.

### **III. PLAINTIFF HAS PROPERLY ALLEGED A VIOLATION FO THE ILLINOIS CONSUMER FRAUD ACT.**

Comcast also seeks dismissal on Count IV on the ground that Plaintiff both “cannot,” and “fails to” allege a violation of the Illinois Consumer Fraud and Abuse Act (the “IFCA,” 815 ILCS 505/1, *et seq.*). (ECF No. 28-1 at 10-13.) Comcast posits several arguments in requesting dismissal, each of which fails.

The IFCA is both a regulatory and a remedial statute to protect various entities, including business persons, against fraud, unfair methods of competition, and other unfair and deceptive business practices. *Robinson v. Toyota Motor Credit Corp.*, 201 Ill.2d 403, 775 N.E.2d 951 (2002). Because the IFCA is in the nature of a remedial statute, courts must construe it liberally

in order to give effect to its purposes. *Id.* (citing *Cripe v. Leiter*, 184 Ill.2d 185, 191, 703 N.E.2d 100 (1998)). The IFCA defines a unfair or deceptive practices as:

"including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact \* \* \* in the conduct of any trade or commerce ... 815 ILCS 505/2 (West 1992).

Section 10(a) of the IFCA creates a remedy for people who suffer damage as a result of a violation of the Act committed by another person, and the elements are: (1) a deceptive act or practice by the defendant; (2) the defendant's intent that the plaintiff rely on the deception; and (3) the occurrence of the deception during a course of conduct involving trade or commerce. *Id.* (citations omitted). A plaintiff may recover for both unfair, and deceptive, conduct. *Id.* (citing *Saunders v. Michigan Avenue National Bank*, 278 Ill. App. 3d 307, 313, 662 N.E.2d 602 (1st Cir. 1996)). In order to state a claim for deceptive practices, the plaintiff must state with particularity and specificity the deceptive acts or practices. *Connick v. Suzuki Motor Co.*, 174 Ill.2d 482, 675 N.E.2d 584 (1996).

Plaintiff alleges in Count VIII that Comcast engaged in deceptive practices by, among other things, participating in "efforts to defend those gaining illegal access to Plaintiff's website from being identified, while at the same time failing to prevent the individuals from continued unlawful entry into the website." (ECF No. 2-2 ¶ 100.) Comcast's first argument is that Plaintiff has not alleged that Comcast's "conduct complained of implicates consumer concerns or that anyone --- consumer or otherwise --- is affected ..." (ECF No. 28-1 at 11.) That argument fails because the "consumer nexus required is that the misconduct either involves trade practices to the market generally, or otherwise implicates concerns for consumer protection. *See, e.g., ASI Acquisition, LLC v. Rayman*, No. 01 C 165, 2002 WL 335311, at \*2 (N.D.Ill. Feb. 28, 2002);

*Downers Grove Volkswagen, Inc. v. Wigglesworth Imports, Inc.*, 190 Ill. App. 3d 524, 546 N.E.2d 33, 40-41 (2d Dist. 1989.) Plaintiff alleged that Comcast's deceptive practices included, among other things, concealing the identities of those gaining illegal access to its websites from identification, while at the same time, failing to prevent the individuals from continued unlawful entry into the website. (ECF No. 2-2 ¶ 100.) Plaintiff alleged that this deception "occurred in the course of conduct involving trade" (*Id.* ¶ 101) and that, as a consequence, Plaintiff's allegations show that this conduct implicates concerns for consumer protection, because Comcast's conduct has allowed the massive and unrelenting hacking into Plaintiff's website. Among other things, Comcast's failure to take conduct to stop hacking by its subscribers allowed massive hacking, estimated at 2,500 hacking attempts per day, to continue unabated. (ECF No. 2-2 ¶ 50.) Defendant's conduct, or failure to act, also contributed to the downloading of 170,000 files, using more than 3.5 terbytes of total bandwidth. (EECF No. 2-2 ¶ 51.) Allowing such massive criminality to continue unchecked directly implicates concerns for consumer protection.

Comcast's argument that Plaintiff did not allege its deceptive practices with the particularly required under Rule 9(b) also fails. Plaintiff attached to its Complaint a list of over 6,000 Internet Protocol addresses that accessed its websites. It alleged with particularity the dates and times that Defendant Smith accessed the website, which led to the investigation yielding the more than 6,000 names. (ECF No. 2-2 ¶¶ 24-26.) It alleged that, despite knowledge of the massive hacking by those individuals, Comcast ran interference for its subscribers who Plaintiff had identified as committing criminal acts. (*Id.* ¶ 35.) Plaintiff alleged that Comcast never instructed its subscribers to stop hacking into its websites, and did not report such criminality to law enforcement. Comcast instead acted as the *de facto* defense counsel for its subscribers, and did everything in its power to prevent Plaintiff from identifying those guilty of

the hacking, while allowing them to continue hacking in exchange for monthly subscriber fees. (ECF No. 2-2 ¶¶ 32-49.) Those allegations specifically identify, with particularity, the acts and omissions of Comcast, when the acts occurred, where and how they occurred. Plaintiff has pled this count with particularity that satisfies Rule 9(9b).

Comcast's final argument, that there is a "litigation privilege" that allows them to facilitate and protect the commission of crimes on the part of their paying customers, likewise fails. (ECF No. 28-1 at 12-13.) Comcast has not "prevailed" in this litigation; it joined in a motion by other ISPs, that resulted a two-sentence Illinois Supreme Order quashing certain subpoenas. Nothing in the Supreme Court's Order suggests that Comcast has the right to facilitate criminal conduct in exchange for a monthly subscriber payment from its customers, and it has not identified a valid "litigation privilege" allowing them to shield their conduct from liability.

**IV. COUNTS VII AND X PROPERLY ALLEGE CONSPIRACY AND AIDING AND ABETTING, RESPECTIVELY.**

Comcast posits a very lengthy and convoluted argument to attack the claim for conspiracy alleged in Count VIII, and the claim for aiding and abetting in Count X. Both arguments fail.

Comcast's primary argument with respect with respect to the claim for conspiracy in Count VII is that Plaintiff did not plead an agreement among the parties. Initially, Comcast argues that there must be underlying torts in order to allege a conspiracy claim. Plaintiff has alleged such torts throughout its Complaint. Furthermore, Comcast suggests that Plaintiff "just allege[d] ... that Comcast as an IP made available and maintained Internet access without reaching understanding with ... other defendants..." (ECF No. 28-1 at 16.) That is a severe misrepresentation of the allegations in Count VII, which state that Comcast was advised that

many of its subscribers were hacking into Plaintiff's website at a massive rate; that Comcast never instructed them to stop, or took action necessary to prevent, such hacking; that, in exchange for continued monthly subscriber payments, Comcast ran interference for them and acted as their *de facto* legal counsel in order to shelter them from liability, and to allow them to continue hacking. (ECF No. 2-2 ¶¶ 98-103.) While Comcast argues that it did not commit an "overt act" in furtherance of the conspiracy, its decision to act as attorneys for its subscribers in order to shield and facilitate their ongoing criminality is clearly an act in furtherance of the conspiracy. Plaintiff has sufficiently pleaded that Comcast reached an explicit agreement with its subscribers that, in exchange for continued monthly subscription payments, Comcast acted to shield and defend them from liability, to conceal their identities from Plaintiff, and to advocate on their behalf while they continued hacking into Plaintiff's websites.

Comcast's argument with respect to the claim for aiding and abetting in Count X grossly misstates Plaintiff's argument. Under Comcast's formulation, it is a passive bystander to the ongoing criminality of its subscribers. In reality, as with the claim for conspiracy in Count VII (which shares the factual allegations of Count X), Comcast has actively allowed, supported and facilitated the ongoing criminal conduct of its subscribers who continue to hack into Plaintiff's websites. Comcast's claim that Plaintiff has failed to allege a causal link between its conduct and the continued hacking is also false. Plaintiff clearly alleged that Comcast's acts and omissions have directly allowed their customers to continue their criminal conduct against Plaintiff.

**V. COUNT IV PROPERLY ALLEGES UNJUST ENRICHMENT.**

Finally, Comcast's argument that Plaintiff has not sufficiently pled unjust enrichment in Count X fails. (ECF No. 28-1 at 19-20.) 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). But, as with the claims at issue here, “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 Ill. App. 3d at 1024-25, 905 N.E.2d 920.

Plaintiff has plead unjust enrichment as a separate count. However, it has also alleged several independent bases to establish a duty on the part of Comcast to act, and that Comcast failed to abide by its duties. Plaintiff's claim is properly supported by the conduct of Comcast in allowing and being complicit in “unlawful or improper conduct,” and it states an appropriate claim for relief in connection with this litigation.

**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.

Respectfully submitted,

LIGHTSPEED MEDIA CORPORATION

DATED: October 1, 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 1, 2012, all counsel of record who are deemed to have consented to electronic serve are being served a true and correct copy of the foregoing document using the Court's CM/ECF system.

**DATED:** October 1, 2012

/s/ Paul A. Duffy