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.	)	No. 3:12-cv-00889-WDS-SCW

EMERGENCY MOTION TO ORDER DEFENDANTS, AT&T AND COMCAST TO PRODUCE LIMITED DISCOVERY PRIOR TO THE RULE 26(f) CONFERENCE

Plaintiff, LIGHTSPEED MEDIA CORPORATION, by and through its undersigned counsel, as and for its Emergency Motion to Order Defendants, SBC INTERNET SERVICES, INC., d/b/a AT&T Internet Services, Ltd. ("AT&T") and COMCAST CABLE COMMUNICATIONS LLC ("Comcast"), to produce limited discovery prior to the Rule 26(f) conference, states as follows:

INTRODUCTION

Plaintiff Lightspeed Media Corporation ("Lightspeed") is a small business that owns and operates subscription-based websites. (*See* Declaration of Steve Jones [hereinafter "Jones Decl."] ¶ 3, attached hereto as Exhibit A.) The integrity of its business depends on preventing unauthorized access to its members-only areas. (*Id.*) In support of this mission, Lightspeed deploys industry-leading anti-hacking systems, namely ProxyPass. (*Id.* ¶ 4.) Yet, no software can

anticipate and protect against every emerging hacking tactic.[1] Lightspeed's websites are heavily targeted by hackers, who are actively hacking into Lightspeed's sites at this very moment. (*Id.*)

The only entities that know the hackers' identities are their Internet Service Providers, AT&T and Comcast ("the Conspiring ISPs"). (*Id.* ¶ 5.) Yet, the Conspiring ISPs are entirely unwilling to divulge the hackers' identities. (*Id.*) They are not even willing to lessen the frequency of the criminal actions that their customers are currently perpetrating against Lightspeed. (*Id.*) Instead, the Conspiring ISPs are providing these criminals with unfettered Internet access—so long, of course, as the criminals continue making subscription payments to the Conspiring ISP's. (*Id.*)

On December 2011, Lightspeed initiated litigation in the Circuit Court of the Twentieth Judicial Circuit, St. Clair County, Illinois, against one of the hacker group's leaders. Compl., *Lightspeed Media Corporation v. John Doe*, No. 11-L-683 (Ill. Cir. Ct. Dec. 14, 2011), attached hereto as Exhibit C. In that action, Lightspeed applied for and received leave from the court to ascertain the hackers' identities. Order, *Lightspeed*, No. 11-L-683 (Ill. Cir. Ct. Dec. 16, 2011), attached hereto as Exhibit D. Among the ISPs that were served with subpoenas were the Conspiring ISPs. At the time they were served with subpoenas, the Conspiring ISPs were merely third-party custodians of records.

[1] *See* Emil Protalinski, *Richard Clarke: China has Hacked Every Major US Company*, Zero Day, March 27, 2012, *available at* http://www.zdnet.com/blog/security/richard-clarke-china-has-hacked-every-major-us-company/11125 (last checked August 16, 2012) (explaining that even high tech, multi-million-dollar corporations cannot prevent hacking from occurring.); Glenn Chapman, *Cyber Defenders Urged to go on the Offensive*, Yahoo! News, July 26, 2012, available at http://news.yahoo.com/cyber-defenders-urged-offense-140023880.html (last checked August 16, 2012) (Former FBI cyber crime unit chief, Shawn Henry, explained that a proactive, instead of simply a reactive, approach needed to be taken to reduce and prevent hacking and other cyber crimes. Black Hat founder Jeff Moss added "I can't print money; I can't raise an army, but I can hire lawyers and they are almost as good. One way to fight the enemy is you just sue them.")

Instead of complying with Lightspeed's subpoenas—and thus conforming to the behavior of the majority of the ISPs—the Conspiring ISPs made a business decision to adopt an obstructionist stance. (Jones Decl. ¶ 5.) Their motive was financial. (*Id.*) As Chief Justice Roberts has recognized, major ISPs profit mightily from high-speed Internet subscriptions. *See TECHNOLOGY; In Court, Verizon Challenges Music Industry's Subpoenas*, N.Y. Times, Sept. 17, 2003 (stating that Internet Service Providers such as AT&T and Comcast "make a lot of money off of piracy . . . People engaged in that activity use the more expensive services that [ISPs] offer."). The information provided by the majority of the ISPs allowed Plaintiff's agents to begin unraveling the conspiracy and decrease instances of hacking. (Jones Decl. ¶ 6.) While many of the identified hackers acknowledged their role and expressed surprise that their identities were subject to discovery, others chose to fight Plaintiff's claims. (*Id.*) Plaintiff is currently litigating its claims against dozens of the hackers that were identified in the original action. (*Id.*)

The Conspiring ISPs went so far at the Illinois Circuit Court level as to raise defenses on behalf of their subscribers arguing, bizarrely, that joinder of the (single) defendant was improper and that the Illinois Circuit Court lacked personal jurisdiction over non-resident members of the hacking conspiracy. Motion to Quash and for Protective Order, *Lightspeed*, No. 11-L-683 (Ill. Cir. Ct. Mar. 19, 2012), attached hereto as Exhibit E. The Circuit Court held that these arguments had no merit, particularly when raised by the conspiring ISPs on behalf of their subscribers. Order Denying Motion to Quash and for Protective Order, *Lightspeed*, No. 11-L-683 (Ill. Cir. Ct. Apr. 12, 2012), attached hereto as Exhibit F. Other courts, including in a recent authoritative opinion by the Hon. Judge Beryl A. Howell of the U.S. District Court for the District of

Columbia, have reached similar conclusions. *AF Holdings LLC v. Does 1-1,058*, No. 12-00048 (D.D.C. Aug. 6, 2012), ECF No. 46, attached hereto as Exhibit B.

In an effort to further delay disclosing their subscribers' identities, the Conspiring ISPs asked the Circuit Court to stay the case so they could certify their arguments for appeal. Motion to Stay, *Lightspeed*, No. 11-L-683 (Ill. Cir. Ct. Apr. 25, 2012), attached hereto as Exhibit G. This request was rejected. Order, *Lightspeed*, No. 11-L-683 (Ill. Cir. Ct. May 21, 2012), attached hereto as Exhibit H. Finally, the Conspiring ISPs submitted a motion for a supervisory order to the Illinois Supreme Court. Motion for Supervisory Order, *AT&T Internet Services, et al. v. Lightspeed Media Corporation*, No. 114334 (Ill. June 12, 2012), attached hereto as Exhibit I. This motion was granted, but the relief granted was limited to reversing an administrative order and ordering certain subpoenas quashed as issued. Order, *AT&T Internet Services*, No. 114334 (Ill. June 27, 2012), attached hereto as Exhibit J. The supervisory order did not dismiss the case, vacate the Circuit Court's order granting leave to issue subscriber identification subpoenas or otherwise hamper Plaintiff's case. *Id.*

In light of the supervisory order, Lightspeed amended its complaint to name the Conspiring ISPs as defendants and name the John Doe defendant. First Amended Compl., *Lightspeed*, No. 11-L-683 (Ill. Cir. Ct. Aug. 3, 2012), attached hereto as Exhibit K. Lightspeed seeks damages against the Conspiring ISPs for the harm associated with the criminal acts of their subscribers after the date on which the Conspiring ISPs were on actual notice of the acts alleged of. *Id.* In the voluminous filings the Conspiring ISPs made at the Circuit Court level, the Conspiring ISPs have never denied that their subscribers were engaging in systematic criminal activity against Lightspeed.

Lightspeed brings this motion on an emergency basis because Lightspeed's business is at a breaking point. In the past two months Lightspeed's systems have been targeted by 9,955 hackers worldwide who have attempted to breach Lightspeed's systems 78,298 times. (Jones Decl. ¶ 8.) The efforts of the Conspiring ISPs have emboldened the hackers, who now believe that they have complete impunity to commit criminal acts against Lightspeed. (*Id.*) The Conspiring ISPs subscribers have permanently destroyed Lightspeed's computer systems, engaged in identity theft against Lightspeed and Plaintiff's counsel, attempted to incite fellow hackers to murder Mr. Jones and even committed bank fraud against Mr. Jones' family. Furthermore, the Conspiring ISPs' aiding and abetting has prevented their criminal subscribers from being put on notice of the pending litigation, and thus their evidence preservation obligations. (*Id.*) As the Conspiring ISPs know, as each day passes Lightspeed's ability to prove its case against the Conspiring ISPs is dramatically lessened. (Jones Decl. ¶ 9.) The Conspiring ISPs' aiding and abetting of their subscribers' criminal acts has gone too far. Plaintiff seeks four forms of emergency relief.

First, Lightspeed requests that this Court order the Conspiring ISPs to immediately transmit a copy of the attached cease and desist notice to the subscribers listed on Exhibit A to the original complaint. *See* Notice, attached hereto as Exhibit L. This basic step will put the Conspiring ISPs' subscribers on notice that they cannot continue to commit criminal acts against Lightspeed with impunity. The Conspiring ISPs have already identified their subscribers and send regular bills to them monthly. (Jones Decl. ¶ 10.) They cannot plausibly claim any burden from this step. In fact, this step will act to lessen the liability that the Conspiring ISPs continue to accrue on a daily basis by way of their aiding and abetting activities.

Second, Lightspeed requests that the Court order the Conspiring ISPs to turn over the identifying information of these subscribers. The Conspiring ISPs have indicated that they have already compiled this information, and disclosing it to Lightspeed will not therefore not present any burden beyond the time associated with putting a stamp on an envelope. (Jones Decl. ¶ 10.)

Third, Lightspeed requests that the Court order the Conspiring ISPs to immediately preserve any and all evidence foreseeably relevant to Lightspeed's case. Both Conspiring ISPs have participated from the sidelines in this case until now, and taken advantage of the legal process without being subject to the obligations applicable to a Federal litigant. As such, the Conspiring ISPs may have already destroyed relevant evidence; Lightspeed requests that the Court order no further destruction.

Fourth, Lightspeed requests that the Conspiring ISPs immediately produce information sufficient to allow Lightspeed to determine the identity of, and then name and serve, the Corporate Representatives identified as Defendants in this lawsuit. Defendants are required to produce that information with their initial disclosures, but there is no reason to allow them to hold onto the information until those initial disclosures. The Conspiring ISPs have exclusive knowledge of the identities of their respective Corporate Representatives, and claims against them cannot proceed until Lightspeed learns who they are.

ARGUMENT

The Court has broad authority under the Federal Rules of Civil Procedure to manage the discovery process. *See, e.g.*, Fed. R. Civ. P. 26(d); 16(b)(3)(B); 16(c)(2)(F). Rule 26(d)(1) explicitly permits a party to seek discovery from any source before the parties have conferred when authorized by a court order. Fed. R. Civ. P. 26(d)(1). The courts in this and other jurisdictions rely on considerations of need and fairness when deciding whether this early

discovery is warranted. *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. O'Connor*, 194 F.R.D. 618, 623 (N.D. Ill. 2000); *accord Lamar v. Hammel*, No. 08-02-MJR-CJP, 2008 WL 370697, at *3 (S.D. Ill. Feb. 11, 2008). Plaintiff has a need for expedited discovery because physical evidence of computer hacking will be destroyed with the passage of time; because hacking by the subscribers of the Conspiring ISPs is ongoing and continuous, necessitating immediate relief; and because this suit cannot proceed without this information. At the same time, Lightspeed's request does not offend traditional notions of fairness and practicality.

Rule 26(d) gives judges broad power to determine the timing and sequence of discovery. Fed. R. Civ. P. 26(d); *see also Crawford-El v. Britton*, 523 U.S. 574, 598 (1998) ("Rule 26 vests the trial judge with broad discretion to tailor discovery narrowly and to dictate the sequence of discovery."). The Federal Rules rely on the discretion of trial judges to tailor the scope, manner, and timing of discovery to the needs of the case and ensure the just, speedy, and inexpensive administration of justice. *See, e.g.*, Fed. R. Civ. P. 16(b)(3)(B); 16(c)(2)(F) (setting forth a trial court's power to manage discovery by modifying the timing and extent of discovery through scheduling and case management orders). Though this Circuit has not articulated a set test or criteria for deciding whether early discovery is warranted, courts in this Circuit in the past has elected to rely on considerations of need and fairness. *Merrill Lynch*, 194 F.R.D. at 623 ("Plaintiff must make . . . showing of the need for the expedited discovery. . . . Courts must also protect defendants from unfair expedited discovery."); *see also Vance v. Rumsfeld*, No. 06-C-6964, 2007 WL 4557812, at *3 (N.D. Ill. Dec. 21, 2007) (balancing "[p]laintiffs' need for information relevant to this litigation against the undeniable hurdles of gathering discovery in Iraq during wartime"); *accord Lamar*, 2008 WL 370697, at *3 ("This Court . . . will rely on

considerations of need and fairness."); *IRC, LP v. McLean*, No. 09-189-JPG-CJP, 2009 WL 839043, at *2 (S.D. Ill. Mar. 31, 2009).

I. THE COURT SHOULD ORDER THE CONSPIRING ISPS TO SUBMIT THE ATTCHED CEASE AND DESIST NOTICE TO THEIR HACKER SUBSCRIBERS

Lightspeed requests that the Court order the Conspiring ISPs to immediately transmit the attached cease and desist notice to the subscribers identified in Lightspeed's initial complaint. The notice will serve at least three critical purposes. First, the notice will—for the first time—put the Conspiring ISPs' subscribers on notice of this litigation. The Conspiring ISPs have taken no identifiable action to put their subscribers on notice of this litigation. (Jones Decl. ¶ 10.) Their subscribers accordingly are not aware that they have to preserve case-critical electronically stored evidence. Second, the notice will instruct subscribers whose Internet accounts have been hijacked by unscrupulous third parties to take measures to secure their Internet accounts. Finally, and most importantly, the notice will cause significant numbers of the Conspiring ISPs' subscribers to actually cease and desist their criminal activity. Until now these subscribers believe they are untouchable and are acting with impunity. The notion that their identities are subject to being revealed will cause the hackers to reconsider the wisdom of committing criminal acts against Lightspeed.

Balanced against Lightspeed's extreme need for this action, the Conspiring ISPs have no plausible argument against providing this notice. First, this situation is of their own making. Issuing this notice would, in part, address the failure of the Conspiring ISPs to take any steps whatsoever to address and stop the widespread and ongoing hacking by their subscribers, and to give some assurance that relevant evidence is not destroyed. (Jones Decl. ¶ 5.) Second, the Conspiring ISPs have already compiled the subscriber information that will be required to

transmit the notices. (*Id.* ¶ 10.) Third, the Conspiring ISPs regularly transmit notices to their subscribers in the ordinary course of business. Finally, if anything, transmitting the attached notice will serve to hedge the liability the Conspiring ISPs continue to accrue on an ongoing basis.

II. THE COURT SHOULD ORDER THE CONSPIRING ISPS TO DISCLOSE THE IDENTITIES OF THE HACKER SUBSCRIBERS

Lightspeed also respectfully requests that this Court direct the Conspiring ISPs to immediately produce to Lightspeed the identities of each and every subscriber of theirs whom Lightspeed has identified as a wrongdoer in this matter. Exs. To Compl., *Lightspeed*, No. 11-L-683 (Ill. Cir. Ct. Dec. 14, 2011), attached as Ex. C.

Because the hacking into and theft from Lightspeed's website is ongoing and continuous, Plaintiff needs to discover the identities of IP subscribers listed in the Complaint in order to take quick actions to prevent further irreparable harm. (Jones Decl. ¶ 7.) Without a way to contact those individuals, Plaintiff will continue to suffer ongoing, continuous injury due to their criminal conduct. (*Id.*) Counsel for the Conspiring ISPs both represented to the St. Clair County Court previously presiding over this matter that they had retrieved the identifying information for each of the IP addresses listed in the Complaint (Jones Decl. ¶ 10), which Lightspeed alleges were associated with individual who hacked into and stole from its site. (Ex. C.) The Conspiring ISPs do not have a reasonable basis to withhold that information from Plaintiff.

While Defendants previously indicated that they would preserve identifying information for their subscribers until this litigation terminates (Jones Decl. ¶ 10), there is no way for either the Plaintiff or this Court to monitor their compliance with those assurances. And there is no valid reason for the Defendants not to release the information immediately. Lightspeed has a clear and undeniable interest in taking any and all steps necessary to prevent criminal activity

from continuing through the use of those IP addresses, including contacting their owners and demanding that they cease and desist from this activity. Furthermore, the Conspiring ISPs do not have a protectable interest that should excuse it from producing the names of its subscribers who used their accounts for criminal conduct against Lightspeed.

There can be no undue burden for the Conspiring ISPs to produce that information, because each has already assembled it, and all either Defendant has to do is forward it to the Plaintiff. (Jones Decl. ¶ 10.) And given the Defendants' admissions that they have already assembled the identifying information, they cannot claim now that producing it is an undue burden under Rule 45. As the U.S. District Court for the District of Columbia recently held in the recent landmark opinion regarding the subject, production of such information is not unduly burdensome in these circumstances. *AF Holdings*, No. 12-00048 (D.D.C. Aug. 6, 2012), ECF No. 46 at 18, attached as Ex. B (rejecting as baseless argument that production of information was overly burdensome after it was already compiled; holding that "[d]espite the fact that the Movant ISPs have already located the requested information, they urge the Court to quash the plaintiff's subpoenas because of misjoinder and lack of personal jurisdiction. This argument is erroneous.")

Lightspeed therefore respectfully requests that this Court direct the Conspiring ISPs to immediately produce to Lightspeed the identifying information for each and every one of their subscribers listed as co-conspirators in the initial complaint filed in this matter. Lightspeed is literally one stamp away from justice on this point.

III. THE COURT SHOULD ORDER THE CONSPIRING ISPS TO PRESERVE OTHER POTENTIALLY RELEVANT EVIDENCE UNTIL AFTER TRIAL

Both of the Conspiring ISPs interposed themselves in this litigation in a vast and concerted effort to prevent Lightspeed from obtaining information as to those subscribers who were guilty of criminal conduct against it. In doing so, they acted as *de facto* legal counsel for their hacker-subscribers, and have prevented Lightspeed from pursuing its valid claims.

Given the obstructionist and dilatory litigation tactics in which both Defendants have (until now) engaged, there is a very clear and immediate risk that discoverable information within their possession, custody and control when this litigation began in December 2011 no longer exists. There is a further risk that the Defendants, given their decision to protect and enable their subscribers' continued criminal activity from claims by Lightspeed, have discarded, and will continue to discard, evidence that is highly relevant to claims against them in the Amended Complaint. That evidence includes, without limitation, information such as communications (or lack of communication) between the Conspiring ISPs and their subscribers instructing the subscribers to discontinue hacking into Lightspeed's website; communications between the Conspiring ISPs regarding to concerted efforts that they have taken in order to stymie Lightspeed's claims; and communications between each Defendant and its respective employees relating to the decision not to comply with subpoenas served in this case.

Defendant clearly has an obligation to provide such evidence to Lightspeed through their initial disclosures in this case. However, given the extreme lengths to which the Conspiring ISPs have already gone in order to avoid complying with subpoenas and other court orders, and to interfere with any attempt on the part of Lightspeed to assert its claims, there is a clear need for the Court to intervene in order to assure that the Conspiring ISPs do not discard evidence

relevant to Lightspeed's claims. Lightspeed therefore respectfully requests that this Court enter an order directing the Conspiring ISPs to preserve any and all evidence potentially relevant to this case, including without limitation any and all evidence relating to their communications with subscribers listed in the Complaint; communications between the Conspiring ISPs; and communications between each Defendant and its respective employees and agents regarding this case.

IV. THE COURT SHOULD ORDER THE CONSPIRING ISPS TO IMMEDIATELY PRODUCE INFORMATION NECESSARY TO IDENTIFY THE CORPORATE REPRESENTATIVE DEFENDANTS

This Court should also order the Conspiring ISPs to either identify, or produce to Lightspeed information sufficient for it to identify, the unnamed Corporate Representative of each entity who is a Defendant in this case, before the Rule 26(f) conference. The Corporate Representative for each entity is, among other thing, the individual ultimately responsible for the decision of each of the Conspiring ISPs to act as *de facto* legal counsel for their subscribers and to prevent Plaintiff from moving forward with its claims.

Courts regularly grant expedited discovery where such discovery will "substantially contribute to moving th[e] case forward." *See, e.g., Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 275–76 (N.D. Cal. 2002); *Living Scriptures*, 2010 WL 4687679, at *1 (granting motion for expedited discovery of Doe Defendants because "without such information this case cannot commence").

Here, the lawsuit cannot proceed against the Corporate Representative Defendants without first discovering their identities. Any delay on the part of Defendants in providing this information increases the chances that the individuals may terminate their employment from Defendants, which may make it substantially more difficult for Lightspeed to locate and serve

them. Although the Conspiring ISPs, through the actions of those Representatives, acted to delay the litigation in this case for nearly nine (9) months, Lightspeed has no basis upon which to learn their identities. Lightspeed needs the Defendants to disclose the identities of the Corporate Representatives described in the Amended Complaint in order for the case against them to move forward. The Court should therefore enter an order at this time directing Defendants to disclose their identities, or to provide Lightspeed with sufficient information to allow it to determine their identities, because doing so will promote judicial economy and allow the case to move forward. Directing Defendants to disclose their Corporate Representatives at this also highly equitable; those Corporate Representatives, without having any of the responsibilities of actually being party litigants, have acted to stymie and delay Lightspeed's attempts to prevent continued theft from their subscribers. Defendants should not be allowed the luxury of further delay, by waiting until after the Rule 26(f) conference, to identify the Corporate Representatives who are Defendants in this case.

CONCLUSION

WHEREFORE, for all of the foregoing reasons, Lightspeed respectfully requests that this Court (i) grant this Emergency Motion; (ii) order the Conspiring ISPs to provide the attached notice letter to each IP address owner of theirs listed in the original Complaint; (iii) order the Conspiring ISPs to disclose the identity of each and every such IP address owner order to Lightspeed; (iv) order the Conspiring ISPs to preserve any and all evidence potentially relevant to Lightspeed's claims; and (v) order the Conspiring ISPs disclose the identities of their respective Corporate Representative named as a Defendant in this case; and (vi) grant any and all further relief that this Court deems to be reasonable and appropriate under the circumstances.

Respectfully submitted,

LIGHTSPEED MEDIA CORPORATION

DATED: August 16, 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 August 16, 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