**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF MISSISSIPPI**
**DELTA DIVISION**

| | | |
|---|---|---|
| COMBAT ZONE CORP. | § | |
| | § | |
| *Plaintiff,* | § | |
| | § | |
| v. | § | Civil Action No. 2:12-cv-00142-MPM-SAA |
| | § | |
| JOHN/JANE DOES 1-2 | § | |
| | § | |
| *Defendants,* | § | |
| | § | |
| | § | |

**MEMORANDUM IN SUPPORT OF RESPONSE TO MOTION FOR EXPEDITED DISCOVERY**

COMES NOW, the Defendants, John/Jane Does 1-2 (hereinafter "Defendants" or "Doe Defendants"), and files this memorandum in support of its response to Plaintiff's Motion for Expedited Discovery ("Motion for Discovery" or "Motion") and would show unto the Court as follows:

## PROCEDURAL POSTURE

The Plaintiff filed its Complaint against the Defendants on Tuesday, August 7, 2012, alleging various copyright infringements following their belief these Defendants duplicated and distributed unauthorized and infringing copies of the Plaintiff's motion picture through BitTorrent technology. Thus, the Plaintiff seeks a Court order allowing it to propound discovery in the form of subpoenas pursuant to 17 U.S.C. § 512(h) on two internet service providers (hereinafter "ISPs") seeking the identity of the Defendants at the internet protocol addresses (hereinafter "IP addresses") listed in Exhibit 1 of Plaintiff's complaint.

## ARGUMENT AND AUTHORITY

### A. Issuance of Subpoenas Under § 512(h) would be improper.

The Plaintiff seeks a subpoena to be issued to the ISP's under 17 U.S.C. § 512(h) for the purpose of identifying alleged copyright infringers. While § 512(h) allows the issuance of subpoenas for the purpose of identifying copyright infringers, Section 512(h) has no application to the case at bar. It has already been held that § 512(h) does not authorize the issuance of a subpoena to an ISP acting solely as a conduit for communications transferred between two internet users, such as persons sharing peer-to-peer files. Recording Industry Association of America, Inc., v. Verizon Internet Services, Inc., 351 F.3d 1229, 1232-34 (D.C.Cir.2003) and AF Holdings, LLC v. Does 1-1, 058, (080612 DCDC, 1:12-cv-00048-BAH). Therefore, a subpoena being issued to the two ISP's identified in this instance would be improper. Id. The Defendant asks this Court to deny the motion for expedited discovery of identification information pertaining to Doe Defendants under 17 U.S.C. § 512(h).

### B. The Federal Rules of Civil Procedure Caution the Court in Permitting Early Discovery in This Case.

When a party files a motion requesting expedited discovery prior to a Rule 26 conference, a majority of courts have deemed that the requesting party must show "good cause" for the court to grant the request. The Fifth Circuit has adopted a two-pronged good cause analysis to help courts determine whether to authorize expedited discovery. A court "must examine the discovery request on [1] the entirety of the record to date, and [2] the reasonableness of the request in light of all the surrounding circumstances." St. Louis Group, Inc. v. Metals and Additives Corp., Inc., et al., 275 F.R.D. 236, 239 (S.D. Tex. 2011). The burden of showing good cause is on the party seeking the expedited discovery. Id. at 240, *citing* Qwest Commc'ns

Int'l, Inc. v. WorldQuest Networks, Inc., 213 F.R.D. 418, 419 (D.Colo.2003). Moreover, the subject matter related to requests for expedited discovery should be narrowly tailored in scope. Id. The Doe Defendants address both prongs mentioned above simultaneously below and hereby submit that in reviewing the entirety of the record to date and considering the reasonableness of Plaintiff's request in light of the surrounding circumstances, its motion for expedited discovery should be denied.

Expedited discovery of identifying information at specific IP addresses may indeed provide Plaintiff with sufficient identifying information to serve process. But it does not follow that the infringing users and the individuals to whom process is served are one and the same. This method of discovery is rife with potential for misidentification. As such, it behooves a court to balance the Plaintiff's legitimate need – a forum in which to seek redress for a wrong – with the First Amendment rights of not just the defendants, but of innocent third parties who might share an IP address with the anonymous infringing user.

The First Amendment protection of free speech covers anonymous speech, and that protection extends to the internet. Mobilisa Inc. v. John Doe 1, et.al, 217 Ariz. 103, 108, 170 P.3 717 (Ariz.App.Div.1 2007), citing Buckley v. American Constitutional Law Found., 525 U.S. 182, 200, 199 S.Ct. 636, 142 L.Ed.2d 599 (1999), and Reno v. ACLU, 521 U.S. 844, 117 S.Ct. 2329, 138 L.Ed.2d 2D 874 (1997). These Defendants recognize those rights are not absolute, and the First Amendment does not extend its free speech protections to copyright infringement, Id., citing Harper & Row Publishers, Inc. v. Nation Enters, 471 U.S. 539, 555-56, 569, 105 S.Ct. 2218, 85 L.Ed.2d 588 (1985), as copyright infringement leads to a lessening of the expectations of First Amendment protections of privacy. Sony Music Entertainment Inc., et al., 326 F.Supp. 2d 556, 566, citing In re Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 256 (D.D.C. 2003),

*rev'd on other grounds*, Recording Indus. Ass'n of America, Inc., 351 F.3d 1229.

Still, courts should take great care to leave those privacy protections in place until an infringing user has been identified. Limited discovery requiring identification of the subscriber at a particular IP address must meet the "reasonable likelihood" standard; that is, the request must show that discovery will likely yield information that will enable Plaintiff to serve process. Sony Music Entertainment Inc., et al., 326 F. Supp. 2d 556 at 566, citing Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578, 80 (N.D. Cal. 1999); Dendrite, 775 A. 2 at 760. But if multiple parties use a single IP address, as is often the case, identifying the name of the address holder could mean Plaintiff serves process on an innocent party rather than the appropriate defendant.

The Plaintiff alleges in its motion that it has sufficiently identified and documented individuals who are real persons it may sue in Federal Court (Expedited Disc. Mot. at 7). However, other than two (2) IP addresses, it fails to produce such documentation or explain how its investigation and identification of these two IP's addresses are believed to be involved in BitTorrent file sharing. Plaintiff's Complaint is wrought with claims that it is "informed and believes" that the fictitiously named Defendants participated in and are responsible for the acts described in the Complaint. It claims these Doe Defendants "shared and republished the same Motion Picture, thus collectively participated in the same swarm sharing Hash from May 17, 2012, through June 9, 2012." (See Complaint at p.17). The Plaintiff claims to have "recorded" each Doe Defendant publishing the Motion Picture via BitTorrent (See Complaint at p.27) and at various times "discovered" and "documented" its copyrighted work being publicly distributed. (See Complaint at p.30). However, the Plaintiff neglects to include its evidence or recordings obtained showing how it is informed that these two unknown Defendants acted in concert with

one another and shares files.

An innocent member of the household might carry the IP address – such as a parent whose minor child accessed the internet through the parent's computer for file-sharing, or a user using a roommate's internet access for the infringing activity. Patrick Collins, Inc. v. John Does 1-23, WL 1019034 at *6 (E.D. Mich. 2012), citing Third Degree Films v. Does 1-3,577, No. C 11 02768 LB, 2011 U.S. Dist. LEXIS 128030, at *4, 2011 WL 5374569 (N.D. Cal. Nov. 4, 2011). Thus, this Court should deny the Plaintiff's request for early discovery, or in the alternate, to require that Plaintiff produce its documentation tracking the alleged infringing activity and order discovery remain sealed until the infringing user has been positively identified.

"Pre-service discovery is akin to the process used during criminal investigations to obtain warrants. The requirement that the government show probable cause is, in part, a protection against the misuse of *ex parte* procedures to invade the privacy of one who has done no wrong. A similar requirement is necessary here to prevent abuse of this extraordinary application of the discovery process…" Seescandy.com, 185 F.R.D. at 579-80. In a cause of action for an offense as socially sensitive as copyright infringement of an adult film, the Defendants ask that the Court make its decision on the motion for expedited discovery in the light of possible misidentification and the stigma attached to pornography that an innocent third party might suffer.

**C. Plaintiff's Request for Identifying Information Will Not Make Identification and Service of Doe Defendants Possible.**

As noted in the preceding section, discovery of Doe Defendants' identifying information does not guarantee service of process of the culpable offender. Courts have begun to acknowledge that information provided by an ISP identifying a subscriber might identify the individual who opened an account at a particular IP address, but does not necessarily identify the infringing user. Patrick Collins, Inc. v. John Does 1-23, 2012 WL 1019034, at 6, citing K. Beech,

Inc. v. John Does 1-41, 2012 U.S. Dist. LEXIS, at *12-13, 2012 WL 773683.

In a 2011 case out of California, doe defendants filed a motion to quash a subpoena for identification of said defendants at an IP address "on the basis of the unreliability of IP and MAC [Media Access Control] address tracing, and the difficulty of determining who is actually using an IP address in light of the fact that some home networks are not secure and that even within the household, it is impossible to determine which approved user is responsible for a particular download." Hard Drive Productions, Inc. v. Does 1-188, 809 F. Supp. 2d 1150, 1153 (N.D. Cal. 2011).

Some critics maintain that software exists that permits users to use false IPs. Similarly, MAC addresses may also be faked; but some claim that tracing of even legitimate MAC addresses can be unreliable because many ISPs do not store MAC address data. Id. Because of the high risk of misidentification in a lawsuit, persuasive authority of court opinion in established case law has said that "…Plaintiff must make some showing that…the discovery is aimed at revealing specific identifying features of the person or entity who committed the act." Seescandy.com, 185 F.R.D. at 579-80.

**D. The Cable Privacy Act Prohibits Disclosure.**

The Doe Defendants are without sufficient information and belief as to whether or not the Internet Service Providers are governed by the Cable Privacy Act and therefore deny said Act applies to this case. The Cable Privacy Act, 47 U.S.C. § 551, authorizes courts to order cable operators to disclose the personally identifying information of subscribers. Subsection (c)(2)(B) stipulates that a cable operator that has received such a court order pertaining to a subscriber must notify that subscriber. Case law favors requiring Plaintiff to undertake to notify Defendants that they are the subject to a subpoena or order of disclosure, and give them "reasonable

opportunity to file and serve opposition to the application." Dendrite, 342 N.J. Super 134, 141, 775 A.2d 756, 760. Following the decision in Mobilisa, some courts have allowed a window of time first for the ISP to notify the subscriber, then time for the subscriber to respond with a motion to quash.

**E. The Court's Decision Will Impact Public Policy.**

The Court's decision regarding Plaintiff's motion for expedited discovery will impact public policy and should be made with several concerns in mind. As detailed in Mobilisa, courts have expressed concern about the "chilling effect" that allowing discovery of an internet user's identity may have on freedom of speech. "Whether the claim is one for defamation or a property-based claim, the potential for chilling anonymous speech remains the same. … [D]isclosure of Doe's identity would expose Doe to the same potential harm. … The potential for chilling speech by unmasking the identity of an anonymous or pseudonymous internet speaker equally exists whether that party is a defendant or a witness." Mobilisa, 217 Ariz. 103 at 111, 170 P.3d 712 at 720.

Additionally, even peer-to-peer file sharing that allegedly infringes copyright may, under some circumstances, enjoy some First Amendment protections if that file sharing makes a statement or manifests a form of creative expression, for example, through a user's choice of musical downloads. Sony Music Entertainment Inc., 326 F. Supp. 2d at 564.

Finally, a balancing test of the interests of each party provides additional considerations. "In our view, requiring the court to balance the parties' competing interests is necessary to achieve appropriate rulings in the vast array of factually distinct cases likely to involve anonymous speech." Mobilisa, 2217 Ariz. 103 at 111, 170 P.3d 712 at 720.

While the Fifth Circuit has adopted the "good cause" test for allowing limited expedited

discovery, the fourth component of a four-prong preliminary injunction test used in a minority of states suggests balancing whether the injury caused to the Plaintiff without expedited discovery is greater than the injury the Doe Defendants will suffer if expedited discovery is granted. Notaro v. Koch, 95 F.R.D. 403 (S.D.N.Y. 1982). Such a balancing test remains a valid consideration in light of the questionable reliability of IP addresses as a method of identifying the infringing user.

Plaintiffs have an obvious and legitimate interest in protecting the copyright of their intellectual property. Juxtaposed to the interests of copyright holders are the interests of these Defendants. "By defining doe defendants as ISP subscribers who were assigned certain IP addresses, instead of the actual Internet users who allegedly engaged in infringing activity, 'Plaintiff's sought-after discovery has the potential to draw numerous innocent internet users into the litigation, placing a burden upon them that weighs against allowing the discovery as designed.'" SBO Pictures, Inc. v. Does 1-3036, 2011 WL 6002620 (N.D. Cal. 2011), citing Hard Drive Prods., Inc. v. Does 1-130, No. C-11-3826 DMR, 2011 U.S. Dist. LEXIS 132449, at *6 (N.D. Cal. Nov. 16, 2011).

In cases such as the one before the Court, which deal with highly sensitive and prejudicial elements such as pornography, the public pursuit of a lawsuit against an individual defendant stands to expose that individual to irreparable harm to the reputation, and possibly more tangible ramifications such as job loss or negatively impact personal relationships. In short, Plaintiff suffers pecuniary loss that, while hurtful to the business, likely does not jeopardize its existence; but the Doe Defendants and possible innocent third parties face damages that could inflict irreparable harm to their reputation, which has no price.

**F. Privacy Interests of Third Parties Balances the Principal of Transparency in the Legal System.**

Should the Court choose to grant Plaintiff's motion for expedited discovery, a limited-

time protection order could balance the need for transparency and Plaintiff's need for identifying information with the privacy interests of innocent third parties. Digital Sin, Inc. v. Does 1-5,698, 2011 WL 5362068 (N.D. Cal. 2011).

Transparency in the legal system is a "central tenet" of public policy. Malibu Media, LLC v. John Does 1-15, 2012 WL 3517374 (2012). To overcome the presumption of transparency, the party requesting a protective order must meet a "good cause" requirement that disclosure will cause a "defined and serious injury," with "articulate reasoning" and citing specific examples of harm or danger posed. Id. at 4.

In the Digital Sin case, a California court offered a compromise that included a limited-extent protective order allowing Digital Sin to file an anonymous motion to proceed with litigation and prohibiting the company from publicly disclosing the Does' identity, with the seal expiring 30 days after Plaintiff received the disclosed identifying information. In turn, the ISP had 30 days to serve Doe with a copy of the subpoena and protective order; and Doe defendants had 30 days from the date of service to file motions. Digital Sin, 2011 WL 5362068 at 5.

In the case at bar, Plaintiff's request allows seven (7) calendar days for the ISP to notify each subscriber of the request for discovery; and it allows each subscriber twenty-one (21) calendar days from the date of notice to file any papers contesting the subpoena. The Doe Defendants respectfully requests that the Court consider requiring that any identifying information released to Plaintiff in discovery remain sealed or reviewed *in camera* by the Court and counsel to the parties until the individual infringing user has been positively identified with a certainty beyond what the IP address provides.

**CONCLUSION**

Defendants respectfully request that the Court deny the Plaintiff's motion requesting

expedited limited discovery prior to a Rule 26 conference. More particularly, the Plaintiff's motion should be denied to the extent it seeks authority to issue a subpoena pursuant to 17 U.S.C. § 512(h). Alternatively, if the Court deems it appropriate to grant Plaintiff's motion under Rule 45, the Doe Defendants request this Court to require that Plaintiff produce its documentation tracking the alleged infringing activity and order discovery remain sealed until the infringing user has been positively identified. Furthermore, absent any legal authority, Plaintiff's request for multi-stage discovery (i.e. depositions, interrogatories, and document requests) should be denied.

Respectfully submitted this the 9th day of October, 2012.

JOHN/JANE DOES 1-2, Defendants

*/s/ Paul Chiniche*

Paul Chiniche (MSB#101582)
Chiniche Law Firm, PLLC.
Post Office Box 1202
1109 Van Buren Avenue
Oxford, Mississippi 38655
Tel: 662.234.4319
Fax: 662.281.8353
Email: pc@chinichelawfirm.com

**ATTORNEY *AT LITEM* FOR DEFENDANTS**

**CERTIFICATE OF SERVICE**

I, PAUL CHINICHE, Attorney *At Litem* for the Defendants, hereby certify that this day I have served a true and correct copy of the above and foregoing pleading upon the following counsel via electronic means using the ECF system:

Thomas G. Jacks, Esq.
Chalker Flores, LLP
14951 N. Dallas Parkway, Suite 400
Dallas, Texas 75254
Email: tjacks@chalkerflores.com

Mark F. McIntosh, Esq.
AT&T Services, Inc.
Suite 05C571, Lenox Park, Blvd. NE
Atlanta, Georgia 30319
Email: Mm5000@att.com

SO CERTIFIED this the 9th day of October, 2012.

*/s/ Paul Chiniche*
PAUL CHINICHE (MSB#101582)