J. Andrew Coombs (SBN 123881)
*andy@coombspc.com*
Annie S. Wang (SBN 243027)
*annie@coombspc.com*
J. Andrew Coombs, A P. C.
517 East Wilson Avenue, Suite 202
Glendale, California 91206
Telephone: (818) 500-3200
Facsimile: (818) 500-3201

Attorneys for Plaintiff Louis Vuitton Malletier, S.A.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA (SAN JOSE)

| | |
|---|---|
| Louis Vuitton Malletier, S.A.,<br><br>Plaintiff,<br>v.<br><br>Akanoc Solutions, Inc., et al.<br><br>Defendants. | Case No.: C 07 3952 JW (HRL)<br><br>OPPOSITION OF PLAINTIFF LOUIS VUITTON MALLETIER, S.A. TO DEFENDANTS' MOTION IN LIMINE NO. 12 TO EXCLUDE DEFENDANTS' SERVERS AND DATA PATHS |

## INTRODUCTION

During the Court ordered inspection of only five of Defendants' servers, according to a protocol established by Magistrate Judge Lloyd after repeated objection and motion practice on behalf of Defendants, [1] Plaintiff's expert made copies of data evidencing Defendants' hosting of scores of websites infringing Plaintiff's intellectual properties, many that appear to be the subject of repeated notice by or on behalf of Plaintiff.

Understandably, Defendants seek to exclude raw data evidencing their massive, persistent and willful activity in aid of such illegal activity. Defendants' Motion in Limine No. 12, however, is properly denied.

[1] See Docket No. 65 (Magistrate Judge Lloyd's Order Compelling Production); Docket No. 76 (This Court's Order Overruling Objections to Order to Compel); Docket No. 124 (Magistrate Judge Lloyd's Order re Discovery Protocol); Docket No. 151 (Magistrate Judge Lloyd's Order Modifying Protocol).

Ignoring for the moment the fact that the data in question was copied from Defendants' own servers pursuant to several Court orders and will be authenticated by Plaintiff's properly identified witnesses, there can be no question concerning the relevance of data demonstrating wholesale hosting of infringing offers of counterfeit Louis Vuitton merchandise and of logs demonstrating their accessibility to the Internet community despite repeated prior notices of such infringing activity transmitted by or on behalf of Plaintiff.

Not only does the evidence pertain to specific websites identified in the First Amended Complaint, to the extent it evidences additional wholesale infringement, that evidence is also relevant as circumstantial evidence of knowledge. Docket No. 167, p. 3:4-6.

Defendants' characterization of the evidence is also misleading. It is the very fact that the data disclosing Defendants' persistent, wholesale hosting of websites was copied from Defendants' own servers that is relevant, as is the evidence of any individual infringement or web log demonstrating access to that material or other isolated file. It is not particularly helpful to the trier of fact to parse the information as Defendants suggest. See e.g., Declaration of J. Andrew Coombs ("Coombs Decl.") at ¶ 2, Ex. A (broader summary is helpful). Moreover, the servers themselves are the foundation for a significant aspect of Plaintiff's expert's testimony demonstrating the website content (and not just the raw data upon which such websites were based). Exclusion of the proferred evidence will make it more difficult for Plaintiff to introduce expert testimony demonstrating the specific websites hosted on Defendants' servers and will unnecessarily prolong proceedings.

That the evidence is "overbroad and overwhelming," irrelevant and cumulative are imagined or a result of Defendants' own pervasive contribution to their users underlying infringing activity.[2]

Overall, Defendants improperly seek to benefit from a situation of their own making: "It is fundamental that a party that does not provide discovery cannot profit from its own failure…and

[2] In this respect it must be noted that the evidence is already limited by virtue of the fact that Louis Vuitton has limited its inspection (and corresponding server data) to but five servers as illustrative of the overall scope of Defendants' contributory infringement.

may be estopped from 'supporting or opposing designated claims or defenses.'" General Atomic Co. v. Exxon Nuclear Co., 90 F.R.D. 290, 1981 U.S. Dist. LEXIS 9374, at *60 (S.D. Cal. April 23, 1981) (quoting Dellums v. Powell, 566 F.2d 231, 235 (D.C. Cir. 1977)). This motion blatantly and unfairly seeks an advantage due to Defendants' own bad faith discovery failures, ignores the fact the evidence was Court ordered and should be denied for these reasons.

**A. The Rules of Evidence Favor Admissibility.**

Motions in limine should be granted sparingly. Alliance Fin. Capital, Inc. v. Herzfeld, 2007 Bankr. LEXIS 4511, at *2 (N.D. Ga. December 17, 2007) citing Sperberg v. Goodyear Tire & Rubber Co., 519 F.2d 708, 712 (6th Cir. 1975); Middleby Corp. v. Hussmann Corp. 1992 U.S. Dist. LEXIS 13138, at *9-10 (N.D. Ill. August 27, 1992). "A pretrial motion in limine forces a court to decide the merits of introducing a piece of evidence without the benefit of the context of trial." CFM Communs., LLC v. Mitts Telecasting Co., 424 F. Supp. 2d 1229, 1233 (E.D. Cal. 2005); see also U.S. v. Marino, 200 F.3d 6, 11 (1st Cir. 1999) (recognizing that proffered evidence can be more accurately assessed in the context of other evidence).

Evidence should be "excluded on a motion in limine only if the evidence is *clearly* inadmissible for any purpose" (internal quotations omitted, emphasis added). Fresenius Med. Care Holdings, Inc. v. Baxter Int'l, Inc., 2006 U.S. Dist. LEXIS 42159, at *14 (N.D. Cal. June 12, 2006). This means Defendants will have to overcome the well established policies favoring admissibility. Daubert v. Merrell Dow Pharms., 509 U.S. 579, 587 (1993) ("The Rules' basic standard of relevance thus is a liberal one."); U.S. v. Curtin, 489 F.3d 935, 942 (9th Cir. 2007) citing Huddleston v. United States, 485 U.S. 681, 688-89 (1988) (the version of Rule 404(b) which became law was intended to "plac[e] greater emphasis on admissibility than did the final Court version."); see also U.S. v. Williams, 445 F.3d 724, 732 (4th Cir. 2006) (relief against admissibility under Rule 403 should be granted sparingly); U.S. v. Fleming, 215 F.3d 930, 939 (9th Cir. 2000) (Rule 403 favors admissibility); U.S. v. Hankey, 203 F.3d 1160, 1172 (9th Cir. 2000) ("the application of Rule 403 must be cautious and sparing"); F.R.E. 102 Adv. Comm. Notes ("rules are to be liberally construed in favor of admissibility" within the bounds of the Rules to achieve goals

of "speedy, inexpensive, and fair trials designed to reach the truth"). Defendants fail to meet their burden as the Court ordered evidence is relevant, unique, and highly probative, especially in light of these policies favoring admissibility.

**B. Defendants Brazenly Object to Evidence That was Produced Pursuant to Court Order and Necessarily Relevant.**

Not only has Magistrate Judge Lloyd and this Court already found the evidence at issue in this motion implicitly relevant, the server data clearly speaks to core elements of Plaintiff's claims, repeatedly denied by Defendants. Evidence of the underlying direct infringement of Plaintiff's copyrights and trademarks is conceded to be the "first" element of Plaintiff's claim for contributory infringement by Defendants. The raw data at issue in this motion contains the basic data from Defendants' servers evidencing such direct infringements.

Evidence of counterfeiting activity and the presence of specific websites on just five of Defendants' servers easily meets the liberal standard of relevance consistently relied upon and cited by the United States Supreme Court. Daubert, 509 U.S. at 587; Tome v. United States, 513 U.S. 150, 174 (1995) (dissenting opinion by Justice Breyer, with whom The Chief Justice, Justice O'Connor, and Justice Thomas joined). While the trial judge is relied upon to keep "the barely relevant, the time wasting, and the prejudicial from the jury," Tome, 513 U.S. at 170 (dissenting opinion) citing United States v. Abel, 469 U.S. 45, 54 (1984), evidence that speaks directly to the elements of the claims at issue and addresses factual points of contention, should be clearly admissible if otherwise acceptable under the Rules. Thus, Fed. R. Evid. 401 and 402 that admit evidence that has "any tendency to make the existence of any fact that is of consequence…more probable or less probable than it would be without the evidence" is a low threshold that Louis Vuitton easily surpasses.

There can be little more relevant to this case for contributory copyright and trademark infringement than evidence of the hosting and continued hosting by Defendants of infringing websites despite notice.[3] Louis Vuitton seeks to introduce evidence of mass counterfeiting on just

[3] Recently, the Federal Trade Commission sued and successfully obtained a preliminary injunction against another San Jose based Internet host for knowingly hosting, participating in and shielding

five of Defendants' over one thousand servers.[4] The evidence offered by Louis Vuitton meets and exceeds the showing of "any tendency." Fed. R. Evid. 401. Louis Vuitton's evidence is not ancillary or inconsequential to its claims, its evidence is fundamental and incriminating.

Even in light of the "broad discretion" trial judges have to determine relevance, the nature of the evidence offered by Louis Vuitton meets and exceeds the standard required by the Rules to address Defendants' contributory infringement and the proliferation of direct counterfeiting and piracy on their servers. Wood v. Alaska, 957 F.2d 1544, 1550 (9th Cir. 1992) (discussed as part of 6th Amendment violation inquiry). The Court should deny Defendants' Motion No. 12 in its entirety.

**C. Defendants' Previously Defeated Arguments Are Properly Denied, Again.**

Without citing a single rule or supporting case, Defendants state that the evidence obtained from their own servers is "voluminous," "inconceivable" and "improper" and demands that Plaintiff "*specifically* identify each of the files" it intends to use. Defendants' Motion No. 12 at pp. 2-3. While repetitive of their recently denied Motion to "Pare Down," Defendants have gone to new extremes by claiming that data, obtained from Defendants' own servers, with the help of Defendants' personnel, can not be authenticated by those with personal knowledge. Defendants' only authority appears to be their unsupportable reliance on the Stored Communications Act, which has been rejected multiple times as inapplicable by this and other courts. *Cf.* Footnote 1 above. Defendants misunderstand the evidence's probative value as in addition to the value of each file or picture, the evidence as a whole is evidence of Defendants' knowledge and of the material

---

illegal activity. FTC v. Pricewert, LLC, et al., 5:09-cv-02407-RMW (N.D. Cal. Filed June 1, 2009) (San Jose). The FTC lists in their contentions that their ISP defendant "…is fully aware that it is hosting huge volumes of illegal, malicious, and harmful content..." and that it "…actively shields its criminal clientele by either ignoring take-down requests issued by the online security community or shifting its criminal clients to other Internet Protocol addresses controlled by [the ISP defendant] so that they may evade detection." Id. at ¶ 14. The factual similarities to the present case are highlighted by the evidence of unlawful activities that appear to have been extracted from Defendants' servers despite Louis Vuitton's take down requests and this lawsuit, suggesting that some form of similar recourse is appropriate here.

[4] It has been cited in various documents that Defendants own and operate 1,400-1,500 servers. Based upon the history of infringing activity isolated to specific IP Addresses, many of which were located on the same server, a sample of only five servers were chosen for inspection and appear to yield evidence of massive amounts of counterfeiting and piracy.

assistance they provide for the underlying activity. Docket No. 167, p. 3: 5-10. For the same reasons as cited by this Court, Defendants' recycled argument should similarly fail as Plaintiff would be prejudiced if not allowed to present this evidence.

The enormity and persistence of Defendants' contributory infringement underlies Plaintiff's allegations and, despite Louis Vuitton's best efforts to educate Defendants as to the infringements occurring on their servers and using their routers, the data obtained from the server inspection definitively shows that Defendants have not responded to Louis Vuitton's warnings. The evidence obtained from Defendants' servers is uniquely situated to address a multitude of misleading arguments proffered by Defendants concerning control, knowledge, and evidence of infringement.

**D. Louis Vuitton's Properly Identified Witnesses Will Authenticate the Data Obtained From the Inspection.**

Plaintiff's experts, and, if necessary, technical personnel engaged in the underlying inspection, will meet any authentication challenge the Defendants elect to mount.

"The bar for authentication is not particularly high…The proponent need not rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be." U.S. v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (citations omitted). The authentication requirement is satisfied with "evidence sufficient to support a finding that the matter in question is what its proponent claims." U.S. v. Pang, 362 F.3d 1187, 1193 (9th Cir. 2004) citing F.R.E. 901(a). A foundation through personal knowledge is unnecessary, a proper foundation "can rest on any manner permitted by Federal Rule of Evidence 901(b) or 902." Id. citing Orr v. Bank of America, 285 F.3d 764, 774 (9th Cir. 2002); see also F.R.E. 901(b) (specifically stating illustrations are listed "not by way of limitation"). The proponent "need only make a prima facie showing of authenticity, as 'the rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.'" U.S. v. Tank, 200 F.3d 627, 630 (9th Cir. 2000). Rule 901(a) defines a standard of admissibility that is rather general or elastic. Moose Creek, Inc. et al. v. Abercrombie & Fitch Co., 331 F. Supp. 2d 1214, 1225 fn. 4 (C.D. Cal. 2004). "A document can be authenticated [under Rule 901(b)(1)]

by a witness who wrote it, signed it, used it, or saw others do so." Orr, 285 F.3d at 774 fn. 8 citing 31 Wright & Gold, Federal Practice & Procedure: Evidence § 7106, 43 (2000).

Plaintiff has identified witnesses that have personal knowledge of the isolation and harvest of data contained on five of Defendants' servers, which was accomplished with the help of Defendants' personnel at Defendants' business location in San Jose. Plaintiff's witnesses will establish that the data retrieved and offered into evidence by Plaintiff came from Defendants' servers based on their personal knowledge. This showing will be sufficient to admit the server data in its entirety under Fed. R. Evid. 901(b)(1); Orr, 285 F.3d at 774 fn. 8 citing 31 Wright & Gold, Federal Practice & Procedure: Evidence § 7106, 43 (2000). This showing is similar to the showing made in Tank, where the government's witness explained how he created the evidence with his computer and stated that the evidence appeared to be an accurate representation of the underlying data. 200 F.3d at 630 (admitting government generated chat room logs). Plaintiff's witnesses can describe the collection process, if contested, and make a more than sufficient showing that the data was verified and is what it purports to be- copies of Defendants' servers.

Another basis for authentication of the data itself is through comparison or cross-reference of printouts of the same domain names identified in other website printout exhibits, and the website materials observed on the servers.[5] Fed. R. Evid. 901(b)(3)-(4). In the context of the Internet, courts consider the distinctive characteristics of a website in making a finding of authenticity. Premier Nutrition, Inc. v. Organic Food Bar, Inc., 2008 U.S. Dist. LEXIS 78353 *16-17, 86 U.S.P.Q.2D (BNA) 1344 (C.D. Cal. March 27, 2008). To the extent the same website was visited on different occasions and was located on one of the five servers copied by the forensics company, the website printouts and the server data should be admitted so the jury can compare the evidence and determine the applicable weight it wishes to afford as to whether or not the website on the server is the same website as that depicted in another of Plaintiff's exhibits, and if it was offering Louis Vuitton product. The website images from the servers support the notion that massive

[5] Plaintiff's expert is exploring the possibility of re-building websites found on Defendants' servers to see what they looked like when they were online. Should this process be successful, Plaintiff will identify and seek to admit those images as exhibits.

amounts of infringement were shielded by Defendants so that these infringing websites could stay online and in business.

Yet another method of authenticating the data is by comparison of "hash values" that are the equivalent of electronic "Bates stamps." "Every digital image or file has a hash value, which is a string of numbers and letters that serves to identify the image or file." United States v. Cartier, 543 F.3d 442, 444 (8th Cir. 2008) ("no two dissimilar files will have the same hash value"). For example, if an image that appears on the server, is copied or sent to another computer, or, is downloaded from the Internet, so long as the image is not changed or altered, it will have the same unique "hash" value. By comparison of a sample of the "hash values" of the server files associated with particular websites with those same files online, the data can be authenticated by this additional means, if necessary. However, this level of "unequivocal" authentication is not required by the Rules.

The fact that there is a sizeable amount of evidence that indicates numerous websites and their apparent infringing activities does not affect the authentication analysis and in no way makes it harder to authenticate. In contrast, it is that much easier to authenticate the data as its inherent reliability is increased when viewed in the context of other infringing material, supporting what appears to be a primary function of the server, to infringe. The jury should decide what weight, if any, it wishes to attribute to the data found, as Plaintiff has made the requisite showing of relevancy and reliability, to have the data introduced at trial. Tank, 200 F.3d at 630 citing United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts . . . would have affected only the weight of the printouts, not their admissibility.").

Furthermore, the data itself is internally authenticating as the server data includes computer generated web logs that appear to indicate when a particular website or file was being accessed online. Plaintiff anticipates that its expert will be able to explain and authenticate the data in whole, more specifically particular website files, how they relate to specific picture files or web logs, and their accessibility online at given points in time. The raw data will facilitate this explanation and help to lay a foundation under these elements of the Plaintiff expert's testimony.

**E. The Server Data is Extremely Probative and There is No Unfair Prejudice to Defendants As The Material Originated From Them.**

Defendants are not entitled to relief under Rule 403.

Relief against admissibility under Rule 403 should be granted sparingly as Rule 403 favors admissibility. Fleming, 215 F.3d at 939; see also Hankey, 203 F.3d at 1172. Some circuits have required that the unfair prejudice be "exceedingly great" while looking at the evidence "most favorable to its proponent, maximizing its probative value and minimizing its prejudicial effect..." U.S. v. Stout, 509 F.3d 796, 806 (6th Cir. 2007). The fact that the court-ordered evidence Defendants seek to exclude came from their own servers should be sufficient to deny this motion. However, Defendants' claims that the probative value of evidence of continued infringement on just five of their over one thousand servers is needlessly cumulative, is confusing, misleading, a waste of time and will cause undue delay, Defendants' Motion No. 12, p. 4:11-16, is without merit and properly denied on those grounds as well.

Prior controlling decisions have acknowledged that "services or products that facilitate access to websites throughout the world can significantly magnify the effects" of infringing conduct and that in certain instances, seeking compliance from providers may be the only meaningful way for copyright holders to protect their rights. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007). In this case, this could not be more true. The scale of the infringing activity, the persistence of that infringing activity and Defendants' part in facilitating that activity, combined with the global nature of the infringements facilitated through Defendants' United States based activity all demonstrate that the imposition of meaningful standards of conduct upon ISPs such as Defendants "may be the only meaningful way" to protect pertinent intellectual property rights. The data from the servers, including website and web log information is highly probative and material and should be admitted.

Defendants' own server data evidencing infringing websites and weblogs evidencing access, is not needlessly cumulative, a waste of time, confusing or misleading. The server data will assist Plaintiff in the introduction of other exhibits demonstrating website printouts and hosting

information and evidence derived from Defendants' own servers will be the most reliable (though not necessarily the only) iteration of such evidence.

"Relevant evidence is inherently prejudicial; but it is only unfair prejudice, substantially outweighing probative value, which permits exclusion of relevant matter under Rule 403. Unless trials are to be conducted as scenarios, or unreal facts tailored and sanitized for the occasion, the application of Rule 403 must be cautious and sparing. Its major function is limited to excluding matter of scant or cumulative probative force, dragged in by the heels for the sake of its prejudicial effect." Hankey, 203 F.3d at 1172. The largely undisputable data that came from Defendants' servers is the best evidence to convey to the jury not only the massive size of the problem and why Defendants' policies, if ever followed, are inadequate, but to help the jury with the ultimate task of ensuring that Defendants can no longer continue to look the other way in finding them liable to Plaintiff for substantial compensatory and punitive damages.

For the foregoing reasons, Defendants' Motion No. 12 should be denied.

Dated: June 22, 2009

J. Andrew Coombs, A Professional Corp.

/s/ J. Andrew Coombs
By: J. Andrew Coombs
Annie S. Wang
Attorneys for Plaintiff Louis Vuitton Malletier, S.A.

**DECLARATION OF J. ANDREW COOMBS**

I, J. Andrew Coombs, declare as follows:

1. I am an attorney at law duly admitted to practice before the Courts of the State of California and the United States District Court for the Northern District of California. I am counsel of record for Plaintiff Louis Vuitton Malletier, S.A. ("Plaintiff" or "Louis Vuitton") in an action styled Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., et al., Case No. C 07 3952 JW. I submit this declaration in support of Plaintiff's Opposition to Defendants' Motion in Limine No. 11. Except as otherwise stated to the contrary, I have personal knowledge of the following facts and, if called as a witness, I could and would competently testify as follows.

2. Attached Exhibit A is a true and accurate copy of Plaintiff's Exhibit 593.31.

3. Attached Exhibit B are true and correct copies of Plaintiff's Exhibit 592, that I am informed and believe were taken of Defendants' internal computer system at the time of the inspection.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed this 22nd day of June, 2009, at Glendale, California.

/s/ J. Andrew Coombs
J. ANDREW COOMBS