

Vandenberg & Feliu, LLP

Attorneys at Law

110 East 42nd Street

New York, New York 10017

Telephone: 212-763-6800

Author's direct dial: 212-763-6809

Fax: 212-763-6810/6814

Ray Beckerman

E-mail: rbeckerman@vanfeliu.com

March 3, 2008

By mail and electronic filing

Hon. Robert M. Levy

Magistrate Judge

U. S. District Court, Eastern District of New York

225 Cadman Plaza East

Brooklyn, NY 11201

Re: UMG Recordings, Inc., et al v. Lindor, 05CV1095(DGT)(RML)

Dear Judge Levy:

This is in reply to the February 27, 2008, letter of Richard L. Gabriel, Esq., attorney for plaintiffs. Due to space constraints, we will (a) ignore the ad hominem attacks and (b) incorporate by reference materials in our reply to the letter of even date of Thomas M. Mullaney, Esq., attorney for SafeNet.

Item 1(b), 24, 25, re, dates, times, locations of services, and persons performing services

It is obvious defendant is entitled to documents relating to these.

Item 2 re compensation

It is fundamental that defendant is entitled to discovery regarding the compensation of an investigator being called by the opposing party. See, e.g. County of Suffolk v. Long Island Lighting Co., 122 F.R.D. 120, 124 (E.D.N.Y. 1988).

Items 3 and 5 re communications with investigator

It is obvious that defendant is entitled to explore documents relating to communications plaintiff and its other representatives have had with the investigator about the subject matter of this case.

Item 23 re CV's, resumes, other documents about background of witnesses

Plaintiffs say nothing about this. Mr. Mullaney implausibly claims to have only one document responsive to this, a resume, and refuses to produce it unless the entire document is stipulated to be confidential (exhibit E). This position is of course ludicrous.

False statements of fact are made in plaintiffs' opposition

Counsel has made several false statements of fact.

* "[T]he information that defendant is seeking is duplicative." This is the opposite of the truth. We specifically instructed Mr. Mullaney NOT to provide the text documents, which were the "information" we had received.

* "[P]laintiffs have already produced... system logs, user logs, trace routes, digital audio files, and voluminous metadata..." This is absolutely untrue. Plaintiffs have produced none of the above. All they have produced is the text documents, which were prepared on March 13, 2006.

* "[M]uch of the information that defendant seeks is precisely the same information that she unsuccessfully sought when this Court denied her motion to compel (Doc. No. 62) and granted plaintiffs' motion for protective order (Doc. No. 75) on March 30, 2007." Plaintiffs devote most of their opposition to this falsehood. This statement is absolutely untrue. As the Court may recall, the motion to compel and protective order motion to which Mr. Gabriel refers related solely to several written agreements entered into between SafeNet and the RIAA on behalf of plaintiffs, which agreements were reviewed by the Court *in camera*. The Court did NOT hold that defendant is not entitled to information about SafeNet's compensation or its investigation; the Court merely held that defendant was not entitled to the agreements. Copies of our motion to compel, and the Court's order denying it, are annexed hereto as exhibit I. The agreements which the Court ruled on are NOT a part of this motion. They were included in item 29 for record purposes, and Mr. Mullaney was specifically instructed that we were not seeking these at this time, but that we would expect him to produce them only to the Court *in camera* (exhibit J). And item 29 was specifically excluded from the within motion to compel.

Backup materials to the text documents (Items # 6-22, 25, 27-28)

We incorporate by reference the several points we made in response to the Mullaney letter concerning the backup materials, and continue with that discussion herein.

Linking the IP address identified by SafeNet to defendant is central to plaintiff's claim. Yet, it is nearly impossible to definitively link an Internet IP address with a personal computing device on the Internet at a given time in the past. Examination of the methods and procedures used by SafeNet to identify the IP address are reasonably likely to reveal flaws in those methods and procedures which would lead to misidentification. SafeNet claims to be able to identify a personal computer at a given time without concurrently monitoring the actual computer and the routing device by which the computer connects to the Internet. This sort of monitoring cannot be done by trusting a FastTrack protocol superpeer server, a Fastrack protocol client application, or any other client application on a remote computer such as those used by SafeNet. It is equally difficult to know whether an IP address has been spoofed by another computer trying to hide illicit activity or infected with malware. (Spoofing is a common technique used by persons trying to hide their computers' identities.) Due to the improbability of absolute identification, defendant requires items 6(a)-(d) to properly defend against fraud or mistake. Examining the methods and procedures used by SafeNet will show any weaknesses in how information is gathered, stored, and analyzed. To not reveal the methods and procedures used by SafeNet is to completely trust a system plaintiffs assert does something nearly impossible to do: provide absolute identification of a computer host on the Internet. In addition to uncovering mistaken or false claims of absolute identification, defendant must be able to examine MediaSentry's methods and procedures for identifying alleged infringed works, downloading files from the Internet, comparing the files to actual copyrighted works, and storing those files. This is relevant because defendant is reasonably likely to find flaws that allow for mistake or fraud, incorrectly attributing the distribution of protected works to her.

Item #7 requests documents concerning the clock time used by SafeNet. Because the IP address in question was assigned dynamically by Verizon, utmost care must be taken to ensure that the clocks of SafeNet's data gathering equipment were synchronized with the DHCP servers at Verizon. Plaintiff alleges Defendant's computer was assigned the IP Address 141.155.57.198 at 6:12:45 EDT on 8/7/2004. This appears to be the time on SafeNet's computers. If those computers are not synchronized in some form with Verizon Internet Services, the clocks between Verizon

and SafeNet will be out-of-synch. The more out-of-synch, the more likely defendant's routing device was not assigned the alleged IP address at the alleged time, making it likely plaintiff has misidentified the computing device in question. Examination of how clocks are set may reasonably lead to show misidentification of defendant.

Item #9 relates to the packet logs. Plaintiff's expert witness has testified that these are the source of the identification of the IP address and are therefore highly relevant. A packet log shows the communications which occur between two network devices, such as a client computer and a server computer communicating over the Internet. Such logs generally list the source device, the destination device, the size of the packet and the date and timestamp of the packet. Packet logs are written out as text files and are easily captured, stored and read. An unaltered packet log can reveal critical information, including what type of data was actually transferred between SafeNet's computers and other network devices on the Internet. Examining packet logs may reveal the accuracy or inaccuracy of plaintiff's identification claims.

Items #10 and 11 request documents and data relating to the identification of the software and hardware used by SafeNet. Software almost always has flaws, or "bugs". Often, the flaws will affect the ability of the software to function accurately, including accurately reporting to which remote devices it connects. Identifying these flaws requires knowing the software, version, platform (operating system and version), hardware and devices connected to the hardware on which the software is installed.

Item #12 asks for the software manuals. In addition to the reasons for #10 and 11, the manuals can show what procedures must be followed in order to properly use the software, and with them examination may reveal that a failure to follow a particular procedure, rather than a flaw in the software itself, may have been the cause of SafeNet's misidentification of defendant.

Item #13 asks for digital copies of the electronic files. It is obvious that we cannot be forced to accept text documents which were prepared during the litigation, for purposes of the litigation, and which can easily have been manipulated and/or altered.

Item #14 asks for digital copies of the peer-to-peer software used for this investigation. Every version of a software product release is different from every other version of that same product. Having the version(s) used by SafeNet is required to test it for flaws that would lead to misidentification of defendant.

We could say much more about why the material requested is necessary to the finder of fact, but due to space constraints we will conclude by saying "Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party" FRCP 26(b)(1) and that neither plaintiffs nor SafeNet have made any type of showing that any of the requests for documents and data defendant has made are in anyway not discoverable. The questions defendant is asking go to the heart of the central evidence supplied by plaintiffs' central, indeed only, fact witness. Accordingly, defendant's motion should be in all respects granted.

Respectfully submitted,

/s/

Ray Beckerman*

cc: Richard L. Gabriel, Esq., Thomas M. Mullaney, Esq.

* We gratefully acknowledge the assistance of student Jonathan Jaffe of the Intellectual Property Law Clinic of the University of San Francisco School of Law in the preparation of this letter.