GAUNTLETT & ASSOCIATES
David A. Gauntlett (SBN 96399)
James A. Lowe (SBN 214383)
Brian S. Edwards (SBN 166258)
Christopher Lai (SBN 249425)
18400 Von Karman, Suite 300
Irvine, California 92612
Telephone: (949) 553-1010
Facsimile: (949) 553-2050
jal@gauntlettlaw.com
bse@gauntlettlaw.com
cl@gauntlettlaw.com

Attorneys for Defendants
Akanoc Solutions, Inc.,
Managed Solutions Group, Inc.
and Steve Chen

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

LOUIS VUITTON MALLETIER, S.A.,

Plaintiff,

vs.

AKANOC SOLUTIONS, INC., et al.,

Defendants.

Case No.: C 07-3952 JW (HRL)

Magistrate Judge Howard R. Lloyd

DECLARATION OF RICHARD GRALNIK IN SUPPORT OF DEFENDANTS' OPPOSITION TO VUITTON'S MOTION FOR MODIFICATION OF ORDER AND SANCTIONS

Date: May 26, 2009
Time: 10:00 a.m.
Ctrm: 2, 5th Floor

I, RICHARD GRALNIK, declare as follows:

PERSONAL BACKGROUND AND QUALIFICATIONS

1. I am an adult resident of Los Angeles County, California. I make this declaration in support of Defendants' opposition to Plaintiff's Motion for Modification of Order for Inspection and Sanctions. I have personal knowledge of the facts set forth below and if called upon as a witness in this action, I could and would competently testify thereto.

2. I have worked in the computer industry for over 25 years in a variety of technical positions including computer programming, networking and network management and information security. I have been a computer forensic investigator since June, 1994, associated with OnlineSecurity, Inc., of Los Angeles, California. I have received over 150 hours of training in computer forensics, electronic discovery, incident response, and network security. I have been designated and qualified as an expert witness in computer forensics in state and federal court and have testified as an expert at depositions, evidentiary hearings, an arbitration and jury trials. A copy of my Curriculum Vitae is submitted herewith as **Exhibit "1530"** and is incorporated fully herein.

3. I have conducted forensic examinations on hundreds of computers and removable devices in support of corporate, civil and government investigations. I have performed evidence preservation, data extraction and replication, electronic discovery, and keyword searches and forensic analysis, providing definitive results by using licensed professional forensic software including Encase from Guidance Software.

COMPANY BACKGROUND

4. OnlineSecurity was founded in 1997. It is a company that, among other things, provides professional services in the areas of computer forensics, incident response, and electronic discovery. Online Security is recognized as a leader in investigative preservation, analysis and reporting and is regularly appointed by court order to perform forensic preservation as well as analysis and storage of computer data.

DIFFICULTY DETERMINING PUBLICLY ACCESSIBLE VS PRIVATE INFORMATION

5. In an unmanaged hosting environment such as that provided by the Defendants, it is highly unlikely that the service provider will have any knowledge of how a website is constructed or how any of its components are named, organized or accessed. How a website is implemented is a function of choices made by the person or people who design it. This goes far beyond the pages that appear in a user's web browser. It includes the underlying applications, data structures, communications, security and other aspects of a functioning website. How all of this is organized, where and how the various components are stored, what they are called, and other criteria are decided by the implementor. Data and images may be stored in files and folders or they may be stored in a database. The text a user sees on their screen may be stored as text or as a picture that contains the text. Webpage content may be static or it may be generated by a program when a user accesses the website and may be a function of selections the user makes during their visit.

6. These variables can make determining what parts of a website may be considered "publicly accessible" or "private" difficult to establish. The user may see information on their computer screen but will almost certainly be prevented from accessing the source of that data. How the files that make up a website are organized is completely at the discretion of whoever builds the website. It may be extremely difficult to isolate the objects that make up what appears in a web browser from other items that operate in the background. Moreover, every website is likely to be different so that no pattern can be assumed or followed to deconstruct one website in relation to another.

7. Another complication is that there is no way to know what other functionality may be provided by whoever is using the hosted site. The website may store personal information about its customers (e.g. credit card information). The site may offer services besides selling something that would entail storing personal information about end users (e.g a dating site). All of this information can be comingled with the website structure in unpredictable ways that make separating one from another difficult at best. It may not even be possible to segregate the various types of data at all.

LIMITING THE SCOPE OF ANALYSIS

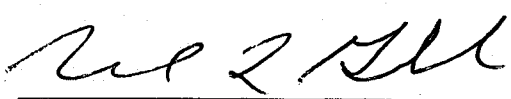
8. In his April 13, 2009 declaration, Mr. Murin, Plaintiff Louis Vuitton's forensic

expert, indicates his intention to search beyond the boundaries of the approved 67 websites when he states, "Executing this search has a near certainty that additional publicly available information outside of the 67 specified websites, will be considered a positive result or "hit" by the software." (Murin Declaration, Page 3: Lines 25-26). Such a search will certainly include areas outside the scope of the 67 websites. Also, Mr. Murin's plan to search indiscriminately for keywords will certainly include areas of the hard drives that are not composed of publicly accessible information. A keyword search will not distinguish between websites or between publicly accessible and private information on its own. The person running the search must select what to search. If that person cannot identify and select appropriate files in advance then the search will examine areas outside the approved scope and there will be no method for selecting approved material after the search either.

NEED FOR COPIES OF FORENSIC IMAGES

9. I understand from his declaration that Joseph Murin and his colleagues from Guidance Software created forensic images of the hard drives from 5 servers at Managed Solutions Group/Akanoc on March 25-26, 2009 (Murin Declaration, Paragraph 5). This type of preservation creates a verifiable copy of the entire contents of a storage device. Such an image becomes a benchmark for all further analysis and both sides in a dispute typically use copies of the same image for that analysis. This eliminates any issues of consistency and commonality of the evidence examined, reported on and presented at trial. Once a storage device is returned to service after being imaged its contents are irreversibly and progressively changed by additional use. The only way for the parties to the matter to make comparisons, draw conclusions and challenge opposing views about the evidence is for both sides to work from identical copies of the evidence.

I hereby declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on April 24, 2009 at Los Angeles, California.



Richard L. Gralnik