

1 **GAUNTLETT & ASSOCIATES**
 David A. Gauntlett (SBN 96399)
 2 James A. Lowe (SBN 214383)
 Preston K. Ascherin (SBN 260361)
 3 18400 Von Karman, Suite 300
 Irvine, California 92612
 4 Telephone: (949) 553-1010
 Facsimile: (949) 553-2050
 5 jal@gauntlettlaw.com
pka@gauntlettlaw.com

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

9
 10 **UNITED STATES DISTRICT COURT**
 11 **NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION**

13 LOUIS VUITTON MALLETIER, S.A.,)	Case No.: C 07-3952 JW (HRL)
)	
14 Plaintiff,)	
)	DEFENDANTS' OPPOSITION TO
15 vs.)	VUITTON'S MOTION FOR A
)	PERMANENT INJUNCTION
)	
17 AKANOC SOLUTIONS, INC., et al.,)	Date: January 25, 2010
)	Time: 9:00 a.m.
18 Defendants.)	Ctrm.: 8, 4th Floor
)	
)	

TABLE OF CONTENTS

Page

I. VUITTON HAS NO RIGHT TO THIS IMPOSSIBLE AND ILLEGAL INJUNCTION..... 1

II. TECHNICAL IMPOSSIBILITY TO COMPLY WITH PROPOSED INJUNCTION..... 1

 A. Vuitton Seeks Broad Injunction Outside An ISP’s Capability to Comply 1

 B. Internet Design Does Not Allow Controls Imagined By Vuitton 2

 1. Internet Transmitted Data Packets Display Only Destination IP Address..... 2

 2. ISP Routers Only Use IP Addresses and Receive No Other Information 3

 3. ISPs Have No Knowledge of Contents of Data Stored or Transmitted..... 3

 4. “Parental Control” Techniques Cannot Block *Incoming* Communication 4

 C. Injunction Requires Non-Existent Technological Abilities 5

 1. “Domain Name Filtering” By ISP Is Impossible 5

 2. Content Filtering By ISP Is Not Feasible 6

 3. ISP Filtering For Images of Protected Marks Is Impossible..... 6

 D. Vuitton’s Discovery Search Illustrates Practical Impossibility 7

 1. Content on a Server Need Not Contain Any Reference to the Website 7

 2. Internet Data Is Transmitted in Fragmented Packets..... 8

 E. Defendants Cannot “Accomplish a Permanent Stop” to Infringing Activity 9

III. VUITTON HAS NOT PROVEN RIGHT TO ANY INJUNCTION 10

 A. Vuitton Does Not Satisfy Any of the Four *eBay* Requirements 10

 1. Vuitton Has Not Suffered and Does Not Face Irreparable Harm 11

 a. No Evidence of Actual Past Harm or Future Harm 11

 b. Possibility of Future Irreparable Harm Improperly Assumed 13

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

2. Legal Remedies (Statutory Damages) Are Adequate..... 13

3. The Balance of Hardships Weighs Heavily in Favor of Defendants..... 14

 a. Vuitton Impermissibly Shifts Burden of Policing to Defendants..... 14

 b. No Practical or Legal Means Exists to Meet Vuitton’s Demands..... 15

4. An Injunction is Against the Public Interest 16

B. Vuitton’s Laundry List of “Abundant Evidence” Is Irrelevant to *eBay* 18

IV. IF VUITTON WERE ENTITLED TO AN INJUNCTION, IT IS NOT THIS ONE 18

 A. The Injunction is Vague and Overbroad in Violation of FRCP 65 18

 B. The Injunction is Unconstitutionally Vague and Overbroad..... 21

 1. The Injunction Is Unconstitutionally Vague For Lack of Scierter 21

 2. The Injunction Is Unconstitutionally Overbroad For Lack of Scierter 22

 C. Compliance with the Injunction Would Be a Criminal Offense..... 23

 D. The Proposed Injunction Violates the Restrictions of the DMCA..... 24

V. CONCLUSION..... 25

TABLE OF AUTHORITIES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Page(s)

FEDERAL CASES

A&M Records v. Napster, Inc.,
284 F.3d 1091 (9th Cir. 2002)..... 16

Au-Tomotive Gold, Inc. v. Volkswagen of America, Inc.,
457 F.3d 1062 (9th Cir. 2006)..... 17

Berry v. Funk,
146 F.3d 1003 (D.C. Cir. 1998) 24

Childress v. Taylor,
798 F. Supp. 981 (S.D.N.Y. 1992)..... 21

eBay Inc. v. MercExchange,
547 U.S. 388 (2006) 1, 10, 18

Fleischmann Distilling Corp. v. Maier Brewing Co.,
314 F.2d 149 (9th Cir. 1963)..... 17

Goldie's Bookstore, Inc. v. Sup. Ct.,
739 F.2d 466 (9th Cir. 1984)..... 12, 14

Granny Goose Foods, Inc. v. Brotherhood of Teamsters,
415 U.S. 423 (1974) 19

Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.
955 F.2d 1143 (7th Cir. 1992)..... 15

Int'l Union, United Mine Workers of America v. Bagwell,
512 U.S. 821 (1994) 21

Klein v. San Diego County,
463 F.3d 1029 (9th Cir. 2006)..... 22

Konop v. Hawaiian Airlines, Inc.,
302 F.3d 868 (9th Cir. (Cal.) 2002)..... 24

Lockheed Martin v. Network Solutions
985 F. Supp. 949 (C.D. Cal. 1997)..... 14

Los Angeles News Service v. Reuters Television Intern., Ltd.,
149 F.3d 987 (9th Cir. (Cal.) 1998)..... 14

MDT Corp. v. New York Stock Exch.,
858 F. Supp. 1028 (C.D.Cal.1994)..... 15

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.,
545 U.S. 913 (2005) 16

1	<i>MGM Studios, Inc. v. Grokster, Ltd.</i> , 518 F. Supp. 2d 1197 (C.D. Cal. 2007).....	10, 13, 16, 21
2		
3	<i>Mulcahy v. Cheetah Learning LLC.</i> 386 F.3d 849 (8th Cir.2004).....	21
4	<i>Price v. City of Stockton.</i> 390 F.3d 1105 (9th Cir.2004).....	22
5		
6	<i>Qualitex Co. v. Jacobson Products, Co., Inc.</i> , 514 U.S. 159 (1995).....	17
7	<i>Regal Knitwear v. N.L.R.B.</i> , 324 U.S. 9 (1945).....	20
8		
9	<i>Rodde v. Bonta.</i> 357 F.3d 988 (9th Cir. 2004).....	13
10	<i>Rosen v. Cascade Intl, Inc.</i> , 21 F.3d 1520 (11th Cir. 1994).....	14
11		
12	<i>Sanders v. Air Line Pilots Assoc.</i> , 473 F.2d 244 (2nd Cir. 1972).....	19
13	<i>Save Our Sonoran, Inc. v. Flowers.</i> 408 F.3d 1113 (9th Cir. 2005).....	13
14		
15	<i>Schmidt v. Lessard.</i> 414 U.S. 473 (1974).....	19
16	<i>Tiffany (NJ) Inc. v. Ebay, Inc.</i> , 576 F. Supp. 2d 463 (S.D.N.Y. 2008).....	15
17		
18	<i>U.S. v. Alaw.</i> 327 F.3d 1217 (D.C. Cir. 2003).....	22
19	<i>Weinberger v. Romero-Barcelo.</i> 456 U.S. 305 (1982).....	10
20		
21		
22	STATE CASES	
23	<i>People v. Freitas.</i> 102 Cal. Rptr. 3d 51 (Cal. App. 2009).....	21
24		
25	DOCKETED	
26	<i>Cuviello v. City of Oakland.</i> No. C-06-5517, 2009 WL 734676 (N.D.Cal. March 19, 2009).....	20
27		
28	<i>Echostar Satellite Corp. v. NDS Group.</i> No. SACV 03-950, 2008 WL 5116513 (C.D.Cal. December 4, 2008).....	20

1 *Microsoft Corp. v. Evans*,
 No. 1:06-cv-01745, 2007 WL 3034661 (E.D. Cal. Oct. 17, 2007)..... 22

3 **FEDERAL RULES AND STATUTES**

4 15 U.S.C. § 1117(c)..... 21
 5 17 U.S.C. § 512(c)(2) 1, 24
 6 17 U.S.C. § 512(j)(1)(A) 25
 7 18 U.S.C. § 2510-2522..... 1, 23
 8 18 U.S.C. § 2510(12) 24
 9 18 U.S.C. § 2511(a)..... 24
 10 18 U.S.C. § 2511(2)(a)(i) 24
 11 18 U.S.C. §§ 2701..... 1, 23
 12 F.R.Civ.P 65 18, 19, 21
 13 F.R.Civ.P 65(d) 1, 18, 19, 20
 14 F.R.Civ.P. 65(d)(1)(C) 19

16 **CONGRESSIONAL RECORDS**

17 H.R. REP. 104-556, at 3 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1074, 1076..... 13
 18 S. REP. NO. 104-177, at 2 (1995) 21
 19 S. REP. 99-541, at 14 (1986) 24

1 Defendants Managed Solutions Group, Inc., Akanoc Solutions, Inc. and Steve Chen hereby
2 oppose plaintiff Louis Vuitton Malletier’s motion for a permanent injunction based on the arguments
3 made here and as made previously [Docket No. 191]

4 **I. VUITTON HAS NO RIGHT TO THIS IMPOSSIBLE AND ILLEGAL INJUNCTION**

5 Vuitton’s motion for injunction reveals a fundamental misunderstanding of the technology,
6 the law and the nature of the business at issue in this case. It is technically impossible for the
7 Defendants to comply with the injunction requirements and Vuitton has shown no way to
8 accomplish what it wants. Vuitton has not proven the requirements of *eBay Inc., v. MercExchange*,
9 547 U.S. 388, 391 (2006) necessary to justify any injunction. The terms of Vuitton’s proposed
10 injunction also violate F.R.Civ.P 65(d) and are unconstitutionally vague and overbroad. Compliance
11 with the terms of the proposed injunction amount to a crime under the Wiretap Act, 18 U.S.C. §
12 2510-2522, and the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* The proposed injunction
13 also violates the injunction restrictions of the Digital Millennium Copyright Act, 17 U.S.C.
14 § 512(c)(2). The Defendants already do everything they can to prevent and end infringement abuses.

15 The proposed injunction is impossible, impractical and illegal and should be denied entirely.

16 **II. TECHNICAL IMPOSSIBILITY TO COMPLY WITH PROPOSED INJUNCTION**

17 **A. Vuitton Seeks Broad Injunction Outside An ISP’s Capability to Comply**

18 Vuitton’s proposed injunction would prohibit the Defendants from “hosting websites that are
19 engaged in the manufacture, import, advertisement, offer for sale, sale, or distribution of
20 Unauthorized Products.” Unauthorized Products are broadly defined as “any unauthorized product
21 which features any of the Louis Vuitton Properties, copies of the Louis Vuitton Properties, or
22 confusingly similar reproductions of the Louis Vuitton Properties.” Those Louis Vuitton Properties
23 are then broadly defined as “Louis Vuitton Copyrights” and “Louis Vuitton Trademarks” that are
24 further defined as fourteen graphic images and three word marks. [Docket No. 188, 2:1-21]. Even
25 disregarding the vagueness and overbreadth of such an order, the requested injunction would require
26 the Defendants in the conduct of their Internet hosting business to electronically: (1) identify
27 “unauthorized products,” (2) that “feature” “copies” or “confusingly similar reproductions” of (3)
28 certain words and fourteen separate graphic images, (4) used by anyone who advertises, sells, offers

1 to sell, or distributes the products on websites, and (5) then prevent the websites' "hosting."

2 Vuitton has not shown how this can be done. Vuitton's demand is technologically
3 impossible, even if it were otherwise entitled to an injunction (and it is not), and despite Vuitton's
4 blithe assertion in its motion. (Docket No. 256, pp. 9:1-3 and 16:14) No Internet Service Provider to
5 Defendants' knowledge and no government agency have ever accomplished what Vuitton demands.
6 Vuitton has not shown that any such injunction has ever been issued. Vuitton's expert witness at
7 trial, Michael Wilson, never testified to any available technology. The proposal is akin to ordering
8 the Post Office not to allow its facilities to be used by anyone offering to sell Vuitton handbags.

9 It is Vuitton's burden to identify and explain what the Defendants should be required to do or
10 prohibited from doing and explain how it should be done. Imaginary ways for the Defendants to
11 protect Vuitton from third-party counterfeiters or shrill demands cannot be enforced by a court. If
12 Vuitton's imaginary technology existed, the governments of the world could stop all objectionable
13 Internet traffic including child pornography, spam, gambling, and political dissent. China would long
14 ago have been able to prevent Internet traffic critical of the Communist Party. Iran would be able to
15 stop organizing of political opponents. Iran has failed. Even China's massive and draconian Internet
16 censorship efforts (unimpeded by free speech or wiretap laws) fail to stop either discussions of
17 Tiananmen Square or the sale of counterfeit merchandise. Vuitton requests an impossible injunction.

18 **B. Internet Design Does Not Allow Controls Imagined By Vuitton**

19 **1. Internet Transmitted Data Packets Display Only Destination IP Address**

20 The Internet's technical design makes impossible the filtering that Vuitton imagines. Internet
21 data is transmitted broken up into "packets" of digital data. Packets ordinarily have no identification
22 on the "outside" except a destination address (a series of numbers). So it is usually not possible to
23 identify information transmitted to or from a particular website by inspecting the available
24 information transmitted with each packet. (Exh "1617"¹ 213:23-215:2; 220:2-222:8) It is also
25 important to remember that a "website" is merely a collection of pages of information stored
26 potentially in multiple servers around the Internet (Exh "1616" 109:1-111:4; 149:4-150:11) End

27 _____
28 ¹Exh "1617," attached to Lowe Decl. are excerpts of the certified trial transcript in this case, Vol. 3, August 20, 2009, testimony of plaintiff's expert witness Michael Wilson.

1 users see a “website” that is a collection of data a creator labels with a domain name. A domain
2 name is routinely issued by one of many domain name registrars; it can be changed quickly. (Exh
3 “1616” 103:12-105:15; 145:11-146:13) Each domain name uses an Internet Protocol (IP) address
4 allowing the routing of data on the Internet through the use of Domain Name Servers. (*Id.* 97:14-
5 99:3) And domain names can easily and quickly change IP addresses. (*Id.* 150:12-21)

6 Data packets do not announce identification of a website or the packet’s contents. Packets,
7 including data from a “website” do not have the domain name or “website name” on the packet.
8 Packets of data to be stored on a server used by a website (potentially including pictures of
9 infringing products) do not have to contain the name of the website where the data will be stored. So
10 it is not useful to scan or even open and inspect a data packet to identify the “website” to which it
11 relates. (*Id.* 141:25-143:25) Consequently, it is pointless to scan Internet transmissions in an effort
12 block transmissions about a particular “website” or domain name.

13 2. ISP Routers Only Use IP Addresses and Receive No Other Information

14 The only information available to an Internet router is an Internet Protocol (IP) address. A
15 router just directs packets to an address, like the Post Office does. So unless some “website” or
16 domain name is tied to a specific IP address based on external information, there is no way to
17 identify it for routing or blocking. (*Id.* 97:7-100:23) An additional problem is that many domain
18 names may use the same IP address. (Exh “1617” 216:25-217:15) So blocking an IP address from
19 being transmitted through an ISP’s system is likely to block many domain names and websites
20 (hundreds or thousands), both legitimate ones and abusive ones. (*Id.* 222:9-223:3) This is equivalent
21 to stopping all mail delivery to an apartment building because it is suspected that one person in the
22 building is conducting some unauthorized business. (*Id.* 226:16-227:5)

23 3. ISPs Have No Knowledge of Contents of Data Stored or Transmitted

24 An ISP has no knowledge of the contents customers place on its servers (Exh “1616”
25 150:22-151:10) any more than a self-storage company knows what its customers put into storage
26 units. An ISP cannot access information on servers rented to customers who have root or
27 administrative access control (*Id.* 114:10-117:15). Even with access, there is no way to identify the
28 contents of its servers except by doing the complex and time consuming searches that Vuitton’s

1 experts did for discovery. Wilson confirmed that would be necessary for Defendants to learn what
2 websites were using its 1,500 servers and 40,000 IP addresses. Without customer permission for
3 inspection, a court order would probably be necessary. (Exh “1617” 249:13-250:321).

4 The undisputed trial evidence established that the Defendants have no technical ability to
5 identify or filter out any Internet traffic based on the names or contents of websites. The only way
6 the Defendants can find out about a website allegedly infringing Vuitton’s trademarks or copyrights
7 is for Vuitton to discover that information by searching for and investigating Internet sellers and then
8 report it to the Defendants. This is why IP owners including Vuitton must police their own marks
9 and works by constantly searching the Internet and its more than 100,000,000 domain names for
10 evidence of infringement. (Exh “1616” 145:11-146:13) Then they can notify ISPs like the
11 Defendants after they have determined what IP address that domain name is using at the time.

12 **4. “Parental Control” Techniques Cannot Block *Incoming* Communication**

13 The ability of a company or a parent to prevent a specific computer from accessing a specific
14 site is entirely unrelated to an ISP seeking to prevent the transmission of infringing content. A
15 program installed on a particular computer can prevent *outgoing* communication to a specific listed
16 website by blocking communication addressed to a specific IP address or searching for a particular
17 keyword (*Id.* 130:21-132:2). This is fundamentally different from trying to keep content from an
18 abusive website from being sent to the computer. It is difficult to prevent even spam from being sent
19 to a computer. While it may be possible to block communication from a specific IP address, an
20 abusive Internet user can disguise or fake a different address, change addresses, send data from a
21 different computer that has been infected with a “botnet” and in many other ways evade controls.

22 An ISP cannot use the “parental control” model to stop infringers from transmitting
23 infringing data through their lines or from storing content on its servers any more than a telephone
24 company could. If AT&T knows someone with a phone number on another network is selling
25 counterfeit handbags, it is a simple matter for AT&T to block its own users’ calls to that external
26 phone number. AT&T, however, cannot prevent its own customers from merely discussing
27 counterfeit handbags or from receiving calls from phone numbers that are unknown to be infringer’s
28 numbers. Likewise, a network’s router can refuse to pass on DNS requests for a domain name

1 known to sell counterfeit handbags, but it is quite another matter for an Internet hosting company to
2 identify content on their servers associated with domains selling counterfeit handbags.

3 **C. Injunction Requires Non-Existent Technological Abilities**

4 **1. “Domain Name Filtering” By ISP Is Impossible**

5 Vuitton incorrectly claims that Defendants expert testified “that domain name filtering is an
6 available and reasonable technology to prevent repeat infringement at the same domain.” Vuitton’s
7 Motion at 5:1-3. Vuitton only cites inadmissible, unidentified and unauthenticated “trial” transcripts
8 that do not identify the witness.² Vuitton has no evidence of that proposition. But the fact is that
9 Defendants don’t receive requests to access any website by name. So there is nothing to “filter.”

10 In reality, user requests for access to websites hosted on an ISP’s servers do not come to the
11 ISP as a request to access a named domain but only as a request to access an IP address. This is an IP
12 address provided to the end user in the moment by the Internet’s Domain Name Service (DNS)
13 resolvers that translates a request to go to a named domain into a series of numbers that the DNS
14 “looks up” to provide the Internet Protocol address with routing directions to the server assigned to
15 that address. Independent registrars and domain name resolvers inform a user’s computer that a
16 desired domain (e.g., “knockoffVuitton.com”) is at that moment using a particular IP address (e.g.,
17 74.125.1.1) associated with a particular server. **Exh “1616”** 97:17-100:23; 102:5-8; 103:12-104:3)
18 So the Defendants do not receive requests to access a particular website or domain name and are
19 never given the domain name or any *reference to a website*. Instead, ISPs only receive requests to
20 access an IP address. Once at that address, the domain name owner’s software re-directs the request.

21 Because the Defendants are not registrars, they have no control over domain names. Because
22 they merely resell in bulk services to connect to the Internet, they do not know what domain names
23 are associated with a particular IP address until and unless a complaint is made about an abusive
24 website allegedly using one of its forty thousand assigned IP addresses. All association between the
25 server’s content and a particular domain happens between a DNS and an end user’s web browsing
26 software; not between Defendants and end users. Defendants cannot “filter” communications by
27

28 ²See Defendants’ Evidentiary Objections to Coombs Declaration and unauthenticated exhibits.

1 domain name because they receive no domain name to filter.

2 **2. Content Filtering By ISP Is Not Feasible**

3 The undisputed evidence is that preventing website abuse (including infringement of
4 trademarks or copyrights) is virtually impossible. It is difficult for an Internet Service Provider to
5 remedy abuse, even if the ISP has received specific information about a website using a particular IP
6 address. (**Exh “1616”**³ 121:5-125:9; 126:4-127:10) Defense expert Richard Gralnik testified that it
7 is not feasible for an Internet Service Provider to do the content filtering that Vuitton demands. (*Id.*
8 144:23-25). Gralnik testified without contradiction to the technical and practical impossibility of an
9 ISP doing content filtering. While it might be *theoretically* possible to search Internet transmissions
10 for simple words, doing so is not practical because the word “Vuitton” for example would be
11 contained *within* packets of data that go through the Defendants’ servers and communications cables.
12 A single message is broken up into multiple packets and transmitted before reassembly as a file.

13 **3. ISP Filtering For Images of Protected Marks Is Impossible**

14 Searching for images of products that might include a Vuitton graphic design is simply
15 impossible. The binary data representing a picture of a handbag, for example, would likely be split
16 up into 20 or 30 data packets and would be transmitted using a variety of Internet protocols. (*Id.* pp.
17 140:6-143:7) But even if one could assemble and internally inspect the contents of all the packets
18 transmitted through the Defendants’ systems, it would impossible to electronically identify a picture
19 as being of an “Unauthorized Product” because the only way to electronically identify such a picture
20 is by using a “checksum” (obtained by determining the numeric value of each pixel on each image
21 and calculating all such pixel values into a single number using a complex algorithm) and then
22 comparing that checksum with the known checksum value of a specific image. But the comparison
23 must be exact, made between a specific individual picture and the checksum of that picture
24 previously provided to the ISP; any variation in the picture (such a cropping it) would produce a new
25 “checksum” and the comparison would fail. Partial images cannot be compared, only a complete
26

27 ³**Exh “1616,”** attached to Declaration of James Lowe in Opposition to Motion for Injunction (“Lowe
28 Decl.”) are excerpts of the certified trial transcript in this case, Vols 8 & 9, August 25, 2009,
testimony of defense expert witness Richard Grelnik.

1 numeric computer file that represents the image. (*Id.* pp. 138:9-139:12; 140:4-143:25) Obviously
2 the Defendants do not have and cannot obtain in advance copies of every possible photograph of
3 every possible counterfeit Vuitton product together with the checksums of each.

4 Since photographs and graphics are transmitted and stored only as numbers, not as physical
5 pictures, filtering pictures transmitted over the Internet (such as a picture of a handbag bearing one
6 of Vuitton’s fourteen graphic designs) is impossible. (*Id.* 132:6-133:2) Pictures are converted into an
7 image format such as JPEG or GIF and then each line of the image is further converted into binary,
8 ASCII, or hexadecimal numbers that require a complex mathematical formula used by a computer
9 program on an end user’s machine for reassembly into something a human can recognize as a
10 picture. Each time a picture is converted into a numeric form it is ultimately translated into zeros and
11 ones then broken up into packets. These binary numbers are unrecognizable by the transmission,
12 routing or storage equipment. Numbers “representing” a picture are stored on a server hard drive at
13 an even lower level as magnetic-charged spaces that the computer reads as ones or zeros. No images
14 of any kind are stored or imprinted anywhere on a server hard drive. (*Id.* 135, 9-24). The low level
15 information is only later converted into JPEG or GIF number sets by specialized programs *after* it is
16 downloaded by an end user to his or her computer. Then yet another program controlling the users
17 computer monitor turns those numbers into a series of pixels that are electronically painted on the
18 user’s screen, for the first time becoming a humanly recognizable picture. (*Id.* pp. 135:25-138:8)

19 So it is not possible to use any electronic or logical filter to know that the stream of numbers
20 includes anything resembling a Vuitton trademark or copyright as Gralnik explained. (*Id.* 131-143)
21 Trial Exhs “1546” and “1547” (attached to Lowe Decl.) illustrate how the same picture of a purse
22 from Louis Vuitton’s website looked entirely different as a set of numbers because one used the
23 JPEG format and the other used the GIF format. This demonstrated that it is technically impossibility
24 of identifying any image transmitted over the Internet to or through the Defendants’ equipment.

25 **D. Vuitton’s Discovery Search Illustrates Practical Impossibility**

26 **1. Content on a Server Need Not Contain Any Reference to the Website**

27 Website content uploaded by customers or customers’ customers to Defendants’ servers need
28 not contain any reference to any domain name. Indeed, website content can lie dormant on a server

1 without *any* domain name associated with it. (**Exh “1616”** 150:22-152:12). Vuitton’s expert,
2 Michael Wilson, testified about the website bigworldshoes.com and Vuitton’s court ordered server
3 search to locate information related to it. Although Mr. Wilson had an exact copy of the server on
4 which the website data was discovered, it took him “ten or twenty” hours using numerous software
5 programs, that were not on the servers, just to rebuild the site as it would have appeared to the public
6 when it was active. (**Exh “1617”** 245:4-248:24; 259:23-260:2). Before rebuilding the site, the
7 website data stored on the server were “just a lot of files” that not even a web host can identify just
8 by looking at them. *Id.* at 248:12-24 and 249:23-250:7. After rebuilding the site, Mr. Wilson was
9 able to “see what it looked like to the outside world.” *Id.* at 262:21-23. Without this step, he would
10 not have been able to identify the “Louis Vuitton part of the bigworldshoes.com web site,” which
11 “had two easy-to-spot characteristics”: (1) the URL for the page with Vuitton type merchandise
12 contained “pcid=16” and (2) the pictures of Vuitton products were all stored in a folder called “thy.”
13 *Id.* at 241:5-242:2; see also **Exh “1559”** (a traffic log for the Vuitton part of bigworldshoes.com
14 testified about by Mr. Wilson (**Exh “1617”** 238:16-242:2) identifying the URL for the Vuitton page
15 only as “/product_list.aspx?pcid=16” and picture URL pictures as, for example,
16 “/pics/qmfncybdyxrlz29yawvz/ufvsu0u=/thy=/2008127182750768.jpg”). Critically, neither of these
17 “easy-to-spot” characteristics reveal anything about the website’s domain name or the actual content
18 of the referenced files. A review of the server files would not reveal that they had anything to do
19 with Vuitton products, counterfeit or otherwise. Only an elaborate and expensive forensic
20 examination of the server hard drive found and identified those files.

21 The file characteristics that were so “informative” were only “easy-to-spot” after a laborious
22 effort by a forensic expert, looking for a single pre-identified website. Only this expert effort finally
23 allowed him to view the server contents in a browser on a different computer and visually identify
24 the Vuitton images. This effort is beyond the technical or practical ability of an ISP operator.

25 **2. Internet Data Is Transmitted in Fragmented Packets**

26 Independently precluding the filtering imagined by Vuitton is the fragmented nature of
27 Internet traffic. When a website operator uploads content to a server, that content does not arrive in
28 any particular sequential order. Instead, the files comprising a websites contents are fragmented into

1 multiple “packets” (Exh “1616” 140:16-143:25) making any electronic filtering impossible. The
2 packets are then distributed from the source computer to the host server out of order and via different
3 routes. *Id.* 98:15-99:20, 100:15-23. The myriad Internet routing devices determine this route by
4 whichever path is most efficient at that particular instant. *Id.* at 98:15-99:20, 100:15-23 and 140:8-
5 143:25. Once all of the packets arrive they are re-assembled. This is analogous to separately mailing
6 pieces of a thousand piece jigsaw puzzle from Los Angeles to New York using many different
7 couriers at different times: some ship by UPS and FedEx on Monday, others go by USPS and DHL
8 on Tuesday, etc. Although the puzzle can be put back together in New York after its thousand
9 pieces arrive, the recipient cannot know what the puzzle depicts just by looking at the pieces as they
10 come in sequentially. Vuitton wrongly assume that Defendants know what a whole puzzle looks like.

11 The only theoretical way to identify the puzzle would be to hold all of the pieces at the post
12 office –here, at the router—then reassemble and examine the puzzle before sending it on. (Exh
13 “1617” 221:17-222:4) Although this might be technically possible with a single file, to do so with
14 every file transmitted to Defendants servers would not be “possible without slowing the network
15 down to the point where almost no data would get through at all.” (Exh “1616” 143:9-25).

16 **E. Defendants Cannot “Accomplish a Permanent Stop” to Infringing Activity**

17 Vuitton demands that Defendants “accomplish a permanent stop to the complained of
18 infringing activity.” (Vuitton’s Motion at 4:1-2) This would require, at the very least, permanently
19 disabling identified domains or websites so they can never appear again – even on *other* ISPs’
20 servers. Vuitton ignores the fact that Defendants are not registrars and so have no control over
21 domain names. (Exh “1616” 104:4-105:25) Some large ISPs, like GoDaddy.com, also happen to be
22 registrars so they have some control over the use of the domain names they rent out. They may also
23 offer web hosting services. (*Id.* 106:1-108:7) As a registrar, if GoDaddy decides a lessee is abusing
24 its domain, it can theoretically “evict” the lessee from the domain. (*Id.* 152:24-154:14) If the content
25 for that domain is also hosted on their servers, they can disable the associated IP address so the
26 lessee cannot simply link it to a new domain through a DNS. Of course, even this does not prevent
27 that party from immediately re-establishing the same content under a different domain, whether on
28 GoDaddy’s, Defendants’ or a third party’s servers. It merely prevents their continued abuse of that

1 domain name. But Defendants are not registrars. They have no control over any domain other than
2 the domain for their own business website. Thus, it is impossible for Defendants to permanently –
3 or even temporarily – shut down any domain they do not own.⁴ Vuitton is asking the impossible.

4 **III. VUITTON HAS NOT PROVEN RIGHT TO ANY INJUNCTION**

5 **A. Vuitton Does Not Satisfy Any of the Four *eBay* Requirements**

6 Vuitton must satisfy a four-part test to be entitled to a permanent injunction but it has not
7 done so. In *eBay Inc. v. MercExchange, LLC*, 547 U.S. 388, 391 (2006), the Supreme Court held
8 that a mere finding of infringement (there, of a patent) does **not** automatically entitle the owner of an
9 intellectual property right to receive an injunction.⁵ Like any other plaintiff, an IP owner must
10 satisfy a four-part test to invoke a federal court’s equitable powers. **Vuitton must prove: (1)**
11 **irreparable injury; (2) the remedies available at law are inadequate to compensate for that**
12 **injury; (3) the balance of hardships favors issuance of an injunction; and (4) the public interest**
13 **would not be disserved by a permanent injunction.** *Id.* at 391. Vuitton’s evidence is inadequate.

14 *Grokster*, quoted the admonishment in *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 312
15 (1982) that “[a]n injunction should issue only where the intervention of a court of equity ‘is essential
16 in order effectually to protect property rights against injuries otherwise irreparable.’ ”⁶

20 ⁴The inherent impossibility of *anyone* permanently disabling a domain or its underlying website was
21 the very premise of the 2008 film “Untraceable.” In that film, even the FBI could not disable
22 “killwithme.com” despite repeatedly disabling the domain’s IP addresses. Although the movie “may
23 be fiction, [] it’s based on fact.” FBI Expert Says Cyber Crime in ‘Untraceable’ Isn’t Far-Fetched,
24 THE NEW CRIMINOLOGIST, 2/11/2008, <http://www.newcriminologist.com/article.asp?nid=2029>.
25 Former FBI cyber-crime specialist E.J. Hilbert and consultant on the film, said the “movie is as
26 technically correct as it can be while still being entertaining” and the “only area . . . fudge[d] is the
27 [faster] time frame.” *Id.*

28 ⁵The *eBay* standard applies in both copyright and Lanham Act trademark cases. *MGM Studios, Inc.*
v. Grokster, Ltd., 518 F. Supp. 2d 1197 (C.D. Cal. 2007) (copyright); *Reno Air Racing Ass’n, Inc. v.*
McCord. 452 F.3d 1126, 1137-38 (9th Cir. 2006) (Lanham Act trademark).

⁶*MGM Studios, Inc. v. Grokster, Ltd.*, 518 F. Supp. 2d at 1208 (“As recently confirmed by the
Supreme Court [in *eBay*], **Plaintiffs must meet their burden with respect to the traditional four-**
part test. . . . Further, the Supreme Court has consistently rejected invitations to replace traditional
equitable considerations with a rule that an injunction automatically follows a determination that a
copyright has been infringed.” Internal quotes and citations omitted).

1 **1. Vuitton Has Not Suffered and Does Not Face Irreparable Harm**

2 **a. No Evidence of Actual Past Harm or Future Harm**

3 At trial, Vuitton provided no evidence of any actual harm, let alone irreparable harm, due to
4 websites listed in its first amended complaint, a fact this Court has acknowledged.⁷ Despite Vuitton’s
5 lamentations about Defendants’ customers’ customers permitting use of services by alleged
6 counterfeiters, Defendants’ proffered evidence that Louis Vuitton sales have dramatically increased
7 during the period of alleged infringement.⁸ Since Vuitton showed no damages over the past several
8 years, it is unreasonably speculative to assert future irreparable harm.

9 Although Vuitton relies on *Grokster* for the proposition that “in run-of-the-mill copyright
10 litigation, [irreparable harm] should not be difficult to establish,” Vuitton does not establish that this
11 case involves “run-of-the-mill” copyright infringement. (Vuitton’s Motion at 7:8-10) Unlike in
12 *Grokster* Defendants do not operate a file-sharing network expressly created to encourage the
13 duplication of copyrighted music *ad infinitum*. Here Vuitton’s motion at 7:22-8:6 claims the
14 “irreparable harm” consists of: (i) Impairment of the exclusivity that allegedly accounts for part of
15 the Vuitton’s premium pricing, (ii) Impairment of Vuitton’s strict control over production,
16 distribution, and marketing of its products, and (iii) The fostering of an international scheme to
17 conceal the identity of counterfeiters and to enable offshore sellers to benefit from ready access to
18 United States consumers. Even if these constituted harm, Vuitton failed to prove its assertions.

19 *Ability to Charge Premium Prices:* Vuitton offered no evidence that its ability to charge a
20 premium for its products has been impaired – by Defendants’ secondary customers or anyone else.
21 Vuitton’s unauthenticated transcript excerpts fail to even identify a witness. But even that alleged

22 _____
23 ⁷(“[T]his is not a case where Vuitton has claimed actual damages, but they are asking for
24 statutory damages. It is fair . . . for a defendant to argue that statutory damages should not be
disproportionate to actual damages.” **Exh “1618”** (trial transcript from 8/25) at 218:9-14.)

25 ⁸[Document Nos. 197-1 (Declaration of James Lowe, attaching financial statements re Vuitton) and
26 197-2 (financial statements)] The proffered financial statements show Louis Vuitton quarter by
27 quarter “double-digit organic revenue growth,” “strong momentum continued” and “excellent
28 performance in Europe, U.S. and Asia, especially China. In the latest quarterly report (Quarter 1,
2009) LVMH reports “good momentum in fashion and leather goods” in Asia, in the U.S. and in
Europe. “Louis Vuitton: Double digit revenue growth. All regions showing positive revenue
growth in Euros. Continued strong momentum in Europe and Asia.” This positive revenue growth
occurred during the worst global recession in memory. Vuitton objected to this evidence.

1 testimony admits that purchasers of cheap replicas are not likely to buy genuine products in the first
2 place. (Vuitton’s Ex. A at 166:1-2). Vuitton has not shown any lost customers or lost sales or any
3 need to lower prices for any reason. Vuitton’s purported witness claimed some of its customers are
4 “genuinely disgusted when they see a cheap imitations [sic] . . . all over the place.” (*Id.* at 166:2-7)
5 Vuitton does not explain how its customers’ disgust over what they *know* are “cheap imitations”
6 harms Vuitton and its *genuine* products. But even “los[t] goodwill and ‘untold’ customers,” is
7 speculative injury that “does not constitute irreparable injury” as a matter of law. *Goldie’s*
8 *Bookstore, Inc. v. Sup. Ct.*, 739 F.2d 466, 472 (9th Cir. 1984).

9 *Ability to Exclude Replicas from Market:* Vuitton has not proved how the marketing Vuitton
10 “replicas” has caused real harm. If their sale is so widespread, it may be that this is good advertising
11 for the real thing because Vuitton’s sales have remarkably increased during a world-wide recession.
12 But even if replicas did cause actual harm, Vuitton does not show how Defendants’ conduct
13 contributes to that harm so as to justify equitable relief or how an injunction could prevent any of
14 that harm; the Defendants neither make or sell or induce the sale of any replicas. Obviously foreign
15 counterfeiters will not be deterred even if the Defendants were forced out of business.

16 *International Scheme Benefiting Offshore Sellers:* Vuitton cites no evidence about its
17 vaguely referenced “international scheme.” This appears to be the product of a Parisian imagination.
18 No evidence shows any global conspiracy causing irreparable harm that this Court can remedy. As
19 briefed in Defendants’ Rule 50(a) Motions [Docket Nos. 209, 210, 244 & 245] regarding the
20 extraterritorial nature of the alleged infringements, *offshore* sellers’ mere access to U.S. consumers
21 does not implicate U.S. law. This legal principle is not negated by Vuitton’s unsupported assertion
22 that “Defendants have enabled countless counterfeiters, most if not all based out of the United
23 States, to carry out their illegal activities.” (Vuitton’s Motion at 8:15-17). Vuitton thus concedes that
24 the counterfeiting activity it wants stopped is outside the U.S. But, contrary to its wishes, such
25 activity is not a violation of U.S. law and is therefore not an “illegal activity” that can justify a U.S.
26 court issuing an injunction. Vuitton must go to China, or perhaps to Congress, for protection from
27 the harm it imagines. But this Court cannot grant the relief it seeks by enjoining anything done in
28 America. Because there is no evidence of any direct infringement in the United States the Court

1 cannot enjoin the Defendants from contributing to it. U.S. law cannot not controlled the activity.

2 **b. Possibility of Future Irreparable Harm Improperly Assumed**

3 Even more speculative and unreasonable is Vuitton’s assumption that potential future, and
4 necessarily unknowable conduct will result in irreparable harm. Vuitton cannot rely on past
5 infringement to support its claim of irreparable harm. The *Grokster* court noted that after *eBay* “there
6 can be no presumption of irreparable harm in the permanent injunction context,” even if a plaintiff is
7 successful on the merits. *Grokster*, 518 F. Supp. 2d at 1211.

8 **“Irreparable harm cannot be established solely on the fact of past**
9 **infringement.** Additionally, it must also be true that the mere
10 likelihood of future infringement by a defendant does not by itself
11 allow for an inference of irreparable harm. ... [T]he onus is on
12 **Plaintiffs to explain why future infringements ... would cause**
13 **irreparable harm.** It cannot be presumed.” *Id.* at 1214-1215 (emphasis
14 added).

15 Vuitton has not even attempted to meet its burden. Vuitton’s proposed solution – making it
16 the sole arbiter of identifying future infringements – is improper. Just because Vuitton sends a
17 complaint about a website does not establish direct infringement, let alone Defendants’ contributory
18 infringement and irreparable injury. (Vuitton’s Ex. G, “Proposed Injunction” at 3:12-4:2)
19 Speculation about future direct infringement by unknown parties (and irreparable injury) cannot be
20 assumed simply because a website uses one of Defendants’ servers. *Id.* at 2:14-21. Vuitton cannot
21 identify yet to be created websites. Vuitton also wrongly assumes that if a particular domain sold
22 infringing goods in the past it must always in the future be presumed to be selling infringing goods.
23 This ignores possible changes in merchandise, website content, or even site ownership.

24 **2. Legal Remedies (Statutory Damages) Are Adequate**

25 Vuitton cannot show that money damages, including available statutory damages, would not
26 adequately compensate it for future infringement. This is not a case of environmental damage or
27 human suffering. See, e.g., *Save Our Sonoran, Inc. v. Flowers*, 408 F.3d 1113, 1120, 1124 (9th Cir.
28 2005) (environmental); *Rodde v. Bonta*, 357 F.3d 988, 999 (9th Cir. 2004) (human suffering). Nor
does it involve “serious health and safety hazards” posed by counterfeit baby food or nuclear reactor
parts. H.R. REP. 104-556, at 3 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1074, 1076. Vuitton sells
fancy handbags. The potential harm posed by future counterfeit Vuitton purses is purely financial.

1 But “[m]ere financial injury . . . will not constitute irreparable harm if adequate compensatory relief
2 will be available in the course of litigation.” *Goldie's Bookstore*, 739 F.2d at 471. Vuitton concedes
3 “damage to valuable intellectual properties is difficult to measure (and a significant part of the
4 rationale for statutory damages in the first place).” (Motion at 8:18-19) Statutory damages are
5 available for copyright and trademark infringement. Statutory damages are intended to compensate
6 for actual injury that is difficult to quantify. Adequate compensatory relief for financial injury will
7 *always* be available to compensate Vuitton. *Los Angeles News Service v. Reuters Television Intern.,*
8 *Ltd.*, 149 F.3d 987, 996 (9th Cir. (Cal.) 1998) (“awards of statutory damages serve both
9 **compensatory** and punitive purposes”) (emphasis added);⁹ *Rosen v. Cascade Intl, Inc.*, 21 F.3d
10 1520, 1527 & n.14 (11th Cir. 1994) (“It is axiomatic that equitable relief is only available where
11 there is no adequate remedy at law; cases in which the remedy sought is the recovery of money
12 damages do not fall within the jurisdiction of equity. . . **There is no indication in this case that a**
13 **legal remedy would not be sufficient to vindicate the shareholders’ rights since they seek the**
14 **payment of damages under federal statutes . . .**”) (emphasis added).

15 Vuitton confuses irreparable harm with merely difficult-to-quantify harm¹⁰ that statutory
16 damages cover. Vuitton offers four sentences, and no evidence, to satisfy its burden of proving the
17 inadequacy of legal remedies. Discussing “compensation” makes no sense without actual harm.

18 3. The Balance of Hardships Weighs Heavily in Favor of Defendants

19 a. Vuitton Impermissibly Shifts Burden of Policing to Defendants

20 Vuitton seeks an unprecedented injunction to shift its burden of policing its intellectual
21 properties to Defendants. Vuitton’s proposed injunction charges Defendants with “accomplish[ing] a
22 permanent stop to the complained of infringing activity.” (Vuitton’s Motion at 4:1-2) But every
23 court considering the issue has held a copyright or trademark owner is responsible for identifying
24 infringement and sending notices to an Internet businesses. *Lockheed Martin v. Network Solutions*

25 _____
26 ⁹ STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS 141 Cong. Rec.
27 S12079-03, S12085) (“The option to elect statutory damages in counterfeit cases ensures that
28 trademark owners are **adequately compensated...**”) (emphasis added)

¹⁰ “[T]he evidence identified additional forms of irreparable harm, admittedly not readily
quantifiable. . . ” (Vuitton’s Motion at 7:20-21)

1 985 F. Supp. 949, 966 (C.D. Cal. 1997) (a domain registrar has “no affirmative duty to police the
2 Internet in search of potentially infringing uses of domain names.”); *Tiffany (NJ) Inc. v. Ebay, Inc.*,
3 576 F. Supp. 2d 463, 518 (S.D.N.Y. 2008) (“[R]ights holders bear the principal responsibility to
4 police their trademarks.”); *MDT Corp. v. New York Stock Exch.*, 858 F. Supp. 1028, 1034
5 (C.D.Cal.1994) (“The owner of a trade name must do its own police work.”); *Hard Rock Cafe*
6 *Licensing Corp. v. Concession Services, Inc.* 955 F.2d 1143, 1149 (7th Cir. 1992) (defendants are
7 not required “to be more dutiful guardians of [trademark plaintiffs'] commercial interests”).

8 It is not the responsibility of any registrar, web host, or ISP to police its servers for infringing
9 material. As other courts have recognized, it is far less burdensome for Vuitton and other rights
10 holders, to police their own intellectual property on the Internet and give DMCA-complaint notices
11 of infringement. Even if Defendants were best situated for some reason to police Vuitton’s
12 intellectual property (and Vuitton has not so shown), it is not the Defendants’ legal responsibility.
13 *Tiffany, Inc.* at 518 (“[E]ven if it were true that eBay is best situated to staunch the tide of trademark
14 infringement to which Tiffany and countless other rights owners are subjected, that is not the law.”)

15 **b. No Practical or Legal Means Exists to Meet Vuitton’s Demands**

16 Vuitton ignores the fact that there is no lawful or practical way for Defendants to monitor
17 information transmitted through or stored on the servers they rent to resellers. With 40,000 IP
18 addresses accessing 1,500 Internet servers constantly, there is no possible or practical means to
19 wiretap communications or monitor content in such a way that can prevent or identify every
20 appearance of a copyrighted work or a trademark associated with the Defendants’ services. In any
21 case, such monitoring would be a criminal offense. Even if Defendants wanted to comply with the
22 injunction, they cannot physically or lawfully do so. This will necessarily lead to unintentional
23 violation of an injunction and the annihilation of Defendants’ business. Vuitton’s Proposed
24 Injunction is Defendants’ ruin, despite all possible efforts to comply with an injunction order.

25 Of course Vuitton makes no bones about the fact that its unprecedented and impossible
26 injunction will force Defendants out of business, apparently to discourage other web hosts from
27 leasing servers to Chinese resellers. Vuitton brazenly argues that if Defendants cannot do the
28 impossible, they must simply go out of business. (Vuitton’s Motion at 9:11-19) Vuitton relies on

1 *A&M Records v. Napster, Inc.*, 284 F.3d 1091 (9th Cir. 2002). But *Napster* did not hold that parties
2 must accomplish the impossible, else discontinue service. In fact, the decision rested on the explicit
3 finding that “more could be done to maximize the effectiveness of [a] new [audio fingerprint]
4 filtering mechanism” that was already in place to filter out *specifically identified* copyrighted works.
5 *Id.* at 1098. This case is nothing like *Napster*. Unlike *Napster’s* audio recognition software, Vuitton
6 has not identified specific means to preemptively filter out “infringing” content. Also, identifying
7 “infringing” content in the form of insignias on random products is quite a different matter from
8 identifying songs. An infringing website can take any number of forms while songs are fixed and
9 recognizable to a business that is established to allow the trading of music. Napster’s entire business
10 purpose was to challenge the copyright laws and it was used almost exclusively for infringing
11 purposes.¹¹ Defendants here are in the legitimate and important business of providing Internet
12 services. Occasional third-party infringement does not justify an injunction. *Metro-Goldwyn-Mayer*
13 *Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 938 (2005) (“Grokster and StreamCast, unlike the
14 manufacturer and distributor in *Sony*, acted with a purpose to cause copyright violations by use of
15 software suitable for illegal use.”) The balance of hardships militates against an injunction.

16 **4. An Injunction is Against the Public Interest**

17 Public interest consideration weighs heavily against Vuitton. Provision of Internet hosting
18 services is not only legitimate, it is necessary to the modern economy. Even if there are some abuses
19 of the technology, Internet hosting and web hosting services provide substantial non-infringing uses
20 that are critical to American business and to the American consumer. Anything that reduces the wide
21 availability of those services harms the public, even if some particular vendor is legitimately helped.

22 Because it will not be technically possible for the Defendants or other ISP’s to comply with
23 the injunction; Vuitton has not attempted to establish how it is technically possible to comply with
24 its injunction. This will lead to a reduction in Internet services to the public (especially for American
25 companies doing business with Asia) because other ISPs will be threatened with similar injunctions

26
27 ¹¹*Grokster*, 518 F. Supp. 2d at 1216 (“StreamCast’s entire business was built around the fundamental
28 premise that Morpheus would be utilized to infringe copyrights, including those owned by
Plaintiffs.”)

1 by Vuitton and others like it. It will not be reasonable for American companies in the Internet
2 hosting business (and the many American companies who supply them goods and services) to
3 continue providing modern Internet communications because of the fear of draconian sanctions
4 being sought against them, regardless of the falsity of allegations of contributory infringement. The
5 public will suffer. The American technology business sector will suffer. Lessened competition will
6 cause prices to increase. American and other companies will tend to go off-shore and harm America.

7 Meanwhile, the public interest is only slightly served, if at all, by providing unreasonable
8 protection from competition to wealthy owners of trademarks and copyrights, while lessening the
9 duty of those companies to police their marks and rights. Vuitton likely wants to put these
10 Defendants out of business in order to use them as object lessons when threatening other ISPa. The
11 injunction would serve as dangerous new precedent against other, similarly situated businesses. This
12 would reduce competition. Reduced competition is undeniably against the public interest, as
13 evidenced by countless state and federal laws designed to promote and protect competition.

14 Vuitton points to no counterbalancing public benefit. This is not surprising. IP laws are not
15 meant to protect the owners of intellectual properties. *Fleischmann Distilling Corp. v. Maier*
16 *Brewing Co.*, 314 F.2d 149, 156 (9th Cir. 1963).¹² Intellectual property laws are meant to protect
17 consumers from confusion as to the source of goods. *Au-Tomotive Gold, Inc. v. Volkswagen of*
18 *America, Inc.*, 457 F.3d 1062, 1067 (9th Cir. 2006) (“The principal role of trademark law is to
19 ensure that consumers are able to identify the source of goods. [*Qualitex Co. v. Jacobson Products,*
20 *Co., Inc.*, 514 U.S. 159, 164 (1995).]”) Intellectual property laws are *not*, as Vuitton’s implies,
21 modern versions of the sumptuary laws of yore, meant to protect wealthy aristocrats from suffering
22 cheaper versions of luxury goods seen in the hands of the great unwashed. Even the most credulous
23 consumer could not be confused as to whether a \$100 handbag advertised a Chinese website as a
24 “replica” is an authentic Vuitton product. Vuitton’s injunction cannot serve the public interest.

25 Vuitton has not established, as it must, all four requirements injunctive relief.
26

27 ¹²“The law is not made for the protection of experts, but for the public- that vast multitude which
28 includes the ignorant, the unthinking and the credulous, who, in making purchases, do not stop to
analyze, but are governed by appearance and general impressions.” (Internal citations omitted).

1 **B. Vuitton’s Laundry List of “Abundant Evidence” Is Irrelevant to eBay**

2 Ignoring the required *eBay* factors, Vuitton instead offers a laundry list of irrelevant
3 purported facts that it claims necessitate an injunction. (Vuitton’s Motion at 3:12-5:10) Its “abundant
4 evidence” consists solely of unidentified and unauthenticated trial transcripts about irrelevancies.
5 The eBay requirements are not established by evidence that: Defendants treated a request for
6 documents regarding a particular site as notice that Vuitton believed the site was engaged in
7 infringement. (Motion at 3:13-15); A reseller had customers with websites on multiple IP addresses.
8 (*Id.* at 4:7-9); An unidentified part-time employee had heard of Microsoft and eBay so referred
9 complaints from them to Defendant Steve Chen. (*Id.* at 4:12-14); Defendants disconnected servers
10 that were used for SPAM. (*Id.* at 4:15-16); Defendants rarely charged resellers a \$25 reconnection
11 fee. (*Id.* at 4:17); A complaint to Soft Layer was “usually enough to solve [a] problem.” (*Id.* at 4:24-
12 27); or It is reasonable for an ISP to respond to abuse complaints in a week. (*Id.* at 5:4-6).

13 Other assertions are not only irrelevant to Vuitton’s *eBay* burden, but misleading: Vuitton
14 suggests that because documents say lovernike.com was unplugged more than once, Defendants are
15 liars. *Id.* at 4:3-5. But that website was unplugged more than once because Defendants chased it
16 down at a different IP address. **Exh “616”** at p.14. Vuitton asserts Defendants’ expert testified that
17 domain name filtering can exclude sites with particular names from servers. (*Id.* at 5:1-3) The
18 purported testimony, at most, only suggests Defendants’ employees can be barred from certain sites.
19 Vuitton’s rambling list is irrelevant, is based on unauthenticated testimony, and mischaracterizes that
20 purported testimony. This list is no substitute for proving each *eBay* factors.

21 **IV. IF VUITTON WERE ENTITLED TO AN INJUNCTION, IT IS NOT THIS ONE**

22 **A. The Injunction is Vague and Overbroad in Violation of FRCP 65**

23 Vuitton’s proposed injunction is vague and overbroad in violation of Federal Rule of Civil
24 Procedure 65 and the Constitution. The injunction does not provide Defendants with adequate
25 guidance and exposes Defendants to contempt charges if an “infringing” website is re-established on
26 their servers – something beyond their control – *even if Defendants are unaware* of the site.

27 A valid injunction must identify specific prohibited or mandated acts. F.R.Civ.P. 65(d)
28 requires that “[e]very order granting an injunction . . . must . . . state its terms specifically[] and

1 describe in reasonable detail . . . the acts restrained or required.” Injunctions must be specific as
2 explained by *Granny Goose Foods, Inc. v. Brotherhood of Teamsters*, 415 U.S. 423, 444 (1974)¹³
3 See *Schmidt v. Lessard*, 414 U.S. 473, 476 (1974) (“The specificity provisions of Rule 65(d) are no
4 mere technical requirements. The Rule was designed to prevent uncertainty and confusion on the
5 part of those faced with injunctive orders, and to avoid the possible founding of a contempt citation
6 on a decree too vague to be understood.”).

7 Vuitton proposes prohibiting Defendants from engaging in two types of conduct.¹⁴
8 Prohibiting the first type of conduct – engaging in counterfeiting – is simply inappropriate. Vuitton
9 has not even alleged such acts by Defendants in the past. Prohibiting the second type of conduct –
10 hosting offending websites – is not shown to be possible. It is technologically impossible for
11 Defendants to preemptively identify and thus exclude websites associated with a particular domain
12 or containing particular content. Thus, the problem with Vuitton’s proposed injunction is more
13 fundamental than a mere failure to “describe in reasonable detail the acts restrained or required.”
14 F.R.C.P. 65(d)(1)(C); see also *Sanders v. Air Line Pilots Assoc.*, 473 F.2d 244, 248 (2nd Cir. 1972).
15 It simply does not restrain or require acts *by Defendants*. Instead, it threatens contempt for unknown
16 acts by unknown *third parties*. The injunction also provides zero guidance for Defendants to
17 identify “copies . . . or confusingly similar reproductions of the Louis Vuitton Properties.” (Proposed
18 Injunction at 2:17-19) Whether a product infringes is a jury issue. But Vuitton demands that
19 Defendants block all “infringement” at their peril.

20 _____
21 ¹³(“[S]erious penalties can befall those who are found to be in contempt of court injunctions.
22 Accordingly, one basic principle built into Rule 65 is that **those against whom an injunction is**
23 **issued should receive fair and precisely drawn notice of what the injunction actually prohibits.**
24 . . . ‘The judicial contempt power is a potent weapon. When it is founded upon a decree too vague to
25 be understood, it can be a deadly one. Congress responded to that danger by requiring that a federal
26 court frame its orders so that those who must obey them will know what the court intends to require
27 and what it means to forbid. . . . **The most fundamental postulates of our legal order forbid the**
28 **imposition of a penalty for disobeying a command that defies comprehension.’”)**

25 ¹⁴(1) “knowingly infringing the Louis Vuitton Properties, either directly or contributorily, in any
26 manner, including generally, but not limited to manufacturing, importing, advertising, offering for
27 sale, selling or distributing any unauthorized product which features any of the Louis Vuitton
28 Properties, copies of the Louis Vuitton Properties or confusingly similar reproductions of the Louis
Properties (‘Unauthorized Products’) or, ” (2) “hosting websites that are engaged in the
manufacture, import, advertisement, offer for sale, sale or distribution of Unauthorized Products.”
(Proposed Injunction at 2:14-21)

1 Parties cannot be “left . . . in the dark as to their duty toward the court.” *Regal Knitwear v.*
2 *N.L.R.B.*, 324 U.S. 9, 15 (1945). Injunctions “are issued to effectuate the purposes of the [law], not
3 for the entrapment of parties, and courts no less than parties desire to avoid unwitting contempts as
4 well as to punish deliberate ones.” *Id.*

5 Just as the Defendants cannot filter out content of offending websites as it is uploaded to their
6 servers, they cannot know about an offending website just because it is stored on their servers. But
7 the Proposed Injunction threatens contempt merely for “hosting websites” without any regard for
8 Defendants’ knowledge, conduct or intent. Defendants cannot act (or refrain from an act) in
9 response to something they do not know about – to say nothing of conduct beyond their control.

10 A similar injunction lacking a scienter requirement was found overbroad in *Echostar Satellite*
11 *Corp. v. NDS Group*, No. SACV 03-950, 2008 WL 5116513, at *4-5 (C.D.Cal. December 4, 2008).
12 NDS would have violated the injunction if it “unwittingly came into possession of a device designed
13 to pirate Echostar’s signal...” *Id.* at *4. “[A]dding a ‘knowing and intentional’ element would . . .
14 more explicitly conform” to the underlying statutory offense required addition of a scienter
15 requirement. *Id.* As in *Echostar*, Defendants would be exposed to contempt if they unwittingly
16 stored an “infringing” domain on their servers. An intentionality requirement more explicitly
17 conforms to the underlying Copyright and Lanham Acts: both of which require scienter. But Vuitton
18 proposes an injunction more overbroad than the one proposed in *Echostar*. The existence of a
19 “device designed to pirate Echostar’s signal” is at least a black and white issue. But the fact-
20 intensive question of whether a domain is “infringing” is left up to Vuitton’s self-serving opinion.

21 Vuitton’s overbroad “obey the law” injunction is unenforceable. Vuitton claims its injunction
22 “merely restates Defendants’ underlying obligation – not to contributorily infringe Louis Vuitton’s
23 rights.” (Proposed Injunction at 10:16-18) This underscores why the injunction does not comply
24 with Rule 65(d). “[N]ot only vague injunctions but also injunctions that simply require a defendant
25 to ‘obey the law’ fail to comply with Rule 65(d).” *Cuviello v. City of Oakland*, No. C-06-5517, 2009
26 WL 734676, at *3 (N.D.Cal. March 19, 2009). In *Cuviello*, the court found provisions that defendant
27 police officers “make only lawful arrests . . . [and] are barred from interfering with Plaintiffs’ free
28

1 speech rights” to be “‘obey the law’ injunctions and thus not enforceable.”¹⁵

2 **B. The Injunction is Unconstitutionally Vague and Overbroad**

3 **1. The Injunction Is Unconstitutionally Vague For Lack of Scienter**

4 Conduct prohibitions can also be unconstitutionally vague for lack of a scienter requirement.
5 *People v. Freitas*, 102 Cal. Rptr. 3d 51 (Cal. App. 2009) similarly rejected probation conditions for
6 this reason. Treatment of probation terms is relevant here because, given the lack of actual harm
7 suffered by Vuitton, the statutory damages claimed here are primarily punitive.¹⁶ So any contempt
8 proceedings in this case are likely to be punitive or quasi-criminal in nature.¹⁷ Probation terms may,
9 like injunctions, “be challenged on the grounds of unconstitutional vagueness and overbreadth.”
10 *Freitas*, 102 Cal. Rptr. 3d at 53. Like injunctions under Rule 65, “[t]o avoid being void for
11 vagueness, a probation condition must be sufficiently precise for the probationer to know what is
12 required of him.” *Id.* at 55. The *Freitas* probation terms prohibited the defendants’ possession of
13 stolen goods or guns and ammunition, whether or not he was aware the goods were stolen, or that he
14 was in possession of guns or ammunition. *Id.* The laws prohibiting possession of stolen property or
15 prohibited possession of a firearm required scienter. So the probation terms were unconstitutionally
16 vague. *Id.* Here neither Vuitton nor the law has any legitimate interest in punishing the Defendants
17

18 ¹⁵See *Grokster*, 518 F. Supp. 2d at 1226 (A permanent injunction must be carefully crafted. “[T]he
19 scope of the injunction should be coterminous with the infringement.” 4 Nimmer & Nimmer, §
20 14.06[C]. This is perhaps partly why “blanket injunctions to obey the law are disfavored.” *Mulcahy*
21 *v. Cheetah Learning LLC*, 386 F.3d 849, 852 n. 1 (8th Cir.2004).)

22 ¹⁶See, e.g., S. REP. NO. 104-177, at 2 (1995) (Congress’ explicit purpose in enacting 15 U.S.C. §
23 1117(c), was to provide “stronger civil **penalties** against counterfeiters, including . . . statutory
24 damage awards of up to \$1,000,000 per mark”) (emphasis added); STATEMENTS ON
25 INTRODUCED BILLS AND JOINT RESOLUTIONS 141 Cong. Rec. S12079-03, S12085) (“The
26 option to elect statutory damages in counterfeit cases ensures that trademark owners and adequately
27 compensated and that **counterfeiters are justly punished.** . . .”) (emphasis added); *Childress v.*
28 *Taylor*, 798 F. Supp. 981, 997 (S.D.N.Y. 1992) (“Given plaintiff’s failure to prove actual [copyright
infringement] damages, the \$30,000 statutory award must be regarded as primarily punitive in
nature.”).

¹⁷See *Int’l Union, United Mine Workers of America v. Bagwell*, 512 U.S. 821, 826, 827-28, 829
(1994) (“Criminal contempt is a crime in the ordinary sense . . . and criminal penalties may not be
imposed on someone who has not been afforded the protections that the Constitution requires of
such criminal proceedings.”; “[A] contempt sanction is considered civil if it is remedial, and for the
benefit of the complainant. But if it is for criminal contempt the sentence is punitive . . . When a
contempt involves the prior conduct of an isolated, prohibited act, the resulting sanction has no
coercive effect.”) (quotations and citations omitted).

1 where they have no knowledge of the presence of an “infringing” site on their servers.

2 **2. The Injunction Is Unconstitutionally Overbroad For Lack of Scienter**

3 Injunctions are unconstitutionally overbroad where they unnecessarily curtail “legitimate
4 activities like walking down the street” or, as here, operating an Internet hosting service.¹⁸ *U.S. v.*
5 *Alaw*, 327 F.3d 1217, 1218, 1221 (D.C. Cir. 2003). *Alaw*, 327 F.3d at 1219 vacated an injunction for
6 the second time for overbreadth. In its first review the court noted: **“the injunction could be**
7 **violated unknowingly because it contained no intent requirement**, and therefore, a defendant
8 might violate the injunction by simply wandering within twenty feet of a covered facility.” After
9 remand, the district court “attempt[ed] to remedy this problem by inserting the word ‘intentionally.’
10 ” *Id.* at 1221. But this was found inadequate.

11 The example we used in our prior opinion remains relevant. We stated
12 then that one of the principal problems with the lack of an
13 intentionality element in the injunction was that, “[w]henver a
14 defendant wandered within twenty feet of a covered facility he would
15 be in technical violation of the injunction.” . . . We then ordered that,
16 “[s]ome element of intent must be inserted in the in-junction in order
17 to avoid curtailing legitimate activities like walking down the street.”
***Id.* As the [modified] injunction could be read, if a defendant was**
intentionally walking down the street and the sidewalk happened
to be within twenty feet of a covered facility, he would violate the
injunction, even if he had no knowledge of the covered facility’s
presence. Thus, the mere insertion of the word “intentionally”
does not address the issue . . .

18 Vuitton’s proposed injunction cannot be saved by the mere insertion of the word
19 “intentionally” or “knowingly.” Otherwise, if Defendants intentionally and knowingly provide
20 Internet hosting services – and one of their servers happens to host an “infringing” website –
21 something beyond their knowledge – they would violate the injunction, even without knowledge.

22 “[A]n injunction must be narrowly tailored ... to remedy only the specific harms shown by
23 the plaintiffs, rather than ‘to enjoin all possible breaches of the law.’ ” *Price v. City of Stockton*, 390
24 F.3d 1105, 1117 (9th Cir.2004).¹⁹ Vuitton is “attempting to enjoin all possible breaches of the law.”

25 _____
26 ¹⁸Constitutional review of an injunction calls for an even more stringent standard than does review
27 of a challenged statute. *Klein v. San Diego County*, 463 F.3d 1029, 1035 (9th Cir. 2006), citing
28 *Madsen v. Women’s Health Center, Inc.*, 512 U.S. 753, 764-65 (1994). (A higher standard is
consistent with the well established rule “ ‘that injunctive relief should be no more burdensome to
the defendant than necessary to provide complete relief to the plaintiffs.’ ” Citations omitted).

¹⁹See *Microsoft Corp. v. Evans*, No. 1:06-cv-01745, 2007 WL 3034661 (E.D. Cal. Oct. 17, 2007),

1 **C. Compliance with the Injunction Would Be a Criminal Offense**

2 The theoretical filtering scheme suggested by Vuitton is not only an impractical obstacle to
3 Internet communications (**Exh “1616”** 143:9-25), the scheme would be a criminal offense.
4 Vuitton’s Proposed Injunction requires Defendants to prohibit “infringing” websites from being
5 uploaded to Defendants’ servers. Vuitton assumes that the Defendants can by unexplained means
6 “filter out” all electronic communications sent to Defendants’ servers concerning certain domain
7 names. This process would require that the Defendants monitor, view or intercept *all* incoming
8 Internet communications using its services in order to identify (and take action against) any
9 communications relating to an “infringing” website. This would require monitoring and inspection
10 of non-public communications, prohibited by wiretap and other laws.²⁰

11 The Defendants cannot lawfully access communications transmitted or stored using its
12 services. Vuitton demands that Defendants screen *all* content to exclude “infringing” websites,
13 without regard for whether data in transit is public or private. Vuitton ignores the fact that data is
14 transmitted in packets that are not accessible to the public. A retail store may publically display
15 some merchandise but that does not permit the landlord to rifle through the store’s mail, accounting
16 records or store rooms searching for evidence of any “infringing” merchandise. Such inspections in
17 America require a court order based on probable cause and executed by law enforcement. Vuitton
18 could not require a landlord of a shopping mall to physically do what it demands the defendants do.

19 Wholly independent of the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*,
20 Defendants are prohibited from monitoring or viewing customer activity except for maintenance
21 purposes or upon issuance of a search warrant. The Wiretap Act, 18 U.S.C. § 2510-2522, imposes
22 criminal punishment for “any person who [] intentionally intercepts, endeavors to intercept, or

23 _____
24 citing *Iconix, Inc. v. Tokuda*, 457 F. Supp. 2d 969, 998-999 (N.D.Cal.2006) (“Plaintiff has succeeded
25 only in showing irreparable harm arising out of **past acts of copyright infringement**. The Court
must therefore **narrowly tailor its preliminary injunction to remedy that particular harm.**”).

26 ²⁰Vuitton incorrectly argues that Defendants monitor all content by legally accessing “publicly
27 accessible websites.” (Vuitton’s Motion at 9:7-10) Actually the Court never rejected the argument
28 that what Vuitton demands is a criminal offense. The Courts’ emphasis that discovery was limited
to publicly available information embraced the idea that something broader can run afoul of wiretap
laws. The Court clarified that “Judge Lloyd specifically limited his order [compelling discovery]
[Docket No. 65] to all **‘publicly posted Internet content.’**” [Docket No. 76 at 2:22-23]

1 procures any other person to intercept or endeavor to intercept, any wire, oral or electronic
2 communication.” 18 U.S.C. § 2511(a). The Act broadly defines “electronic communication” as

3 **any transfer of signs, signals, writing, images, sounds, data, or**
4 **intelligence of any nature transmitted in whole or in part by a**
5 **wire, radio, electromagnetic, photoelectronic or photooptical**
6 **system** that affects interstate or foreign commerce.

7 18 U.S.C. § 2510(12) (emphasis added). This encompasses electronic uploads to Defendants’
8 servers. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. (Cal.) 2002) (data transfers to
9 servers storing web page content constitute “electronic communications”).²¹ 18 U.S.C. §
10 2511(2)(a)(i) applies to parties maintaining the system over which electronic communications travel:
11 (“[P]rovider of wire communication service to the public **shall not utilize service observing or**
12 **random monitoring** except for mechanical or service quality control checks.”) Defendants simply
13 cannot screen communications to or from their servers for particular content without committing a
14 crime any more than telephone switchboard operators can screen call content for illegal activity.²²

14 **D. The Proposed Injunction Violates the Restrictions of the DMCA**

15 Vuitton’s proposed injunction also violates the restrictions on injunctions in Section 512(j) of
16 the Digital Millennium Copyright Act (“DMCA”). The law limits the form and scope of injunctive
17 relief against Internet Service Providers who qualify for safe harbor under the Act.²³ The DMCA
18 prohibits the Court from entering an injunction against copyright infringement except for “**providing**
19 **access to infringing material** or activity residing **at a particular online site** on the provider's
20 system or network. . . . providing access to a subscriber or account holder of the service provider's

21 _____
22 ²¹S. REP. 99-541, at 14 (1986) (“As a general rule, a communication is an electronic communication
23 protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be
24 characterized as containing the human voice. **Communications consisting solely of data**, for
25 example . . . **are electronic communications**. This term also includes electronic mail, digitized
26 transmissions, and video teleconferences.”) (emphasis added).

25 ²²Even the “switchboard operator” exception is narrow, covering only “activity which is a necessary
26 incident to the rendition of [] service.” See also *Berry v. Funk*, 146 F.3d 1003, 1010 (D.C. Cir.
27 1998): (“Congress recognized switchboard operators, when connecting calls, inevitably would
28 overhear a small part of a call, but the exception permitting them to use that content is limited only
to that moment or so during which the operator must listen to be sure the call is placed.”)

27 ²³MSG’s and Akanoc’s November 26, 2007 Interim Designations of Agent to Receive Notification
28 of Claimed Infringement filed with the U.S. Copyright Office, **Exhs. “54” and “55,”** made them
eligible for the protections of the DMCA. See 17 U.S.C. § 512(c)(2).

1 system or network who is engaging in infringing activity and **is identified in the order . . .** [or]
2 prevent[ing] or restrain[ing] infringement of copyrighted material specified in the order of the court
3 **at a particular online location**, if such relief is the least burdensome to the service provider among
4 the forms of relief comparably effective for that purpose.” 17 U.S.C. § 512(j)(1)(A) (emphasis
5 added). Vuitton’s proposed injunction meets none of these requirements.

6 These Congressional restrictions on injunctions against ISPs implicitly acknowledge the
7 realities of the on-line world and the fact that Internet hosts cannot “accomplish a permanent stop to
8 complained-of infringing activity” [p. 4:1-2] or “insure [sic] that [infringement] is not resumed on
9 servers or using facilities owned by [the ISP].” [p. 3:10-11] Section 512(j) also recognizes that
10 rights-holders such as Vuitton must police their own works on the Internet. ISPs cannot be, and *are*
11 not, expected to do the policing job for rights holders, including even Louis Vuitton.

12 Vuitton asserts that the DMCA “safe harbor” does not apply to the Defendants.²⁴ Even
13 though the DMCA designations were filed after the initial alleged infringements, they are effective
14 now and the DMCA controls future injunctions. Managed Solutions Group and Akanoc operate a
15 single ISP business and properly publish required information.

16 Defendants cannot “accomplish a permanent stop” to infringement. If this were remotely
17 possible, there would be no infringing activity anywhere in the world. There would be no spam,
18 phishing, child porn, or any other conduct that governments around the world try to stop. There
19 would be no “ddos” attacks, no botnets, no hacking of computer systems, etc.

20 **V. CONCLUSION**

21 Vuitton’s proposed injunction is entirely unjustified. The terms are impossible, impractical
22 and illegal. The Defendants can do no more than take action after each Vuitton notification.

23 Dated: January 4, 2010

GAUNTLETT & ASSOCIATES

By: /s/James A. Lowe
David A. Gauntlett
James A. Lowe
Preston K. Ascherin
Attorneys for Defendants
Akanoc Solutions, Inc.,
Managed Solutions Group, Inc., and Steve Chen

28 ²⁴Relying only on unidentified and unauthenticated mystery testimony to which Defendants object.