GAUNTLETT & ASSOCIATES
David A. Gauntlett (SBN 96399)
James A. Lowe (SBN 214383)
Brian S. Edwards (SBN 166258)
18400 Von Karman, Suite 300
Irvine, California 92612
Telephone: (949) 553-1010
Facsimile: (949) 553-2050
jal@gauntlettlaw.com
bse@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) Hon. Magistrate Judge Howard R. Lloyd **DECLARATION OF JAMES A. LOWE IN OPPOSITION TO VUITTON'S ADMINISTRATIVE MOTION RE DISCOVERY ORDERS**

I, JAMES A. LOWE, declare:

1. I am an attorney duly licensed to practice law before this Court and am a partner in the law firm of Gauntlett & Associates, counsel of record for defendants Managed Solutions Group, Inc., Akanoc Solutions, Inc. and Steve Chen ("Defendants").

2. I have personal knowledge of the facts stated in this Declaration and could testify competently to them if called upon as a witness.

3. This declaration is submitted in support of Defendants' opposition to plaintiff Louis Vuitton Malletier, S.A.'s ("LV") Administrative Motion Re Inspection Protocol.

4. Attached as **Exhibit "A"** is a letter sent by me to Vuitton's counsel on October 24, 2008.

5. Attached as **Exhibit "B"** is the August 7, 2008 Court Order, Docket No. 76.

6. Attached as **Exhibit "C"** is a letter sent by me to Vuitton's counsel on August 8, 2008.

7. Attached as **Exhibit "D"** is a letter sent by me to Vuitton's counsel on September 5, 2008.

8. Attached as **Exhibit "E"** is a letter sent by me to Vuitton's counsel on September 19, 2008.

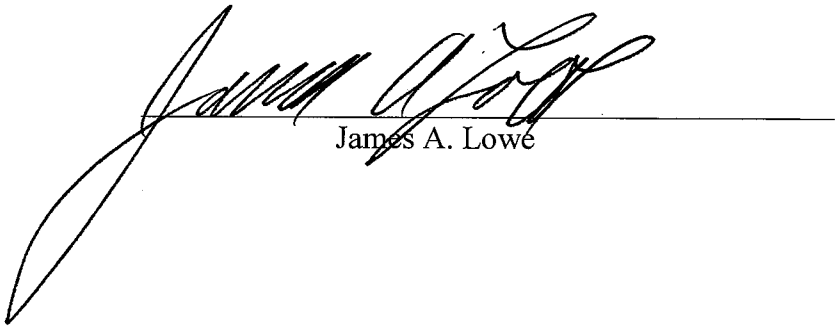
9. Attached as **Exhibit "F"** is a letter sent by my associate, Christopher Lai, at my direction, to Vuitton's counsel on September 26, 2008.

10. Attached as **Exhibit "G"** is a letter sent by me to Vuitton's counsel on October 13, 2008.

11. Attached as **Exhibit "H"** is a letter sent by me to Vuitton's counsel on August 22, 2008.

12. Attached as **Exhibit "I"** is a letter sent by me to Vuitton's counsel on November 12, 2008.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed at Irvine, California on November 12, 2008.



James A. Lowe

EXHIBIT A

GAUNTLETT & ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

October 24, 2008

CONFIDENTIAL SETTLEMENT COMMUNICATION

This communication constitutes an offer of compromise and is subject to the provisions of California Evidence Code § 1152, Rule 408 of the Federal Rules of Evidence and all other similar rules.

VIA E-MAIL
annie@coombspc.com

Annie Wang, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.*
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

- **Objections to Vuitton's Proposed Server Inspection Protocol**

Dear Ms. Wang:

In furtherance of our effort to agree with Louis Vuitton to a protocol for inspection of Internet servers at our clients' facilities, as required by Judge Ware's Order of August 7, 2008, we provide the following information for use by your forensic computer consultant and your office to identify potential servers to inspect and to develop a practical protocol. This information, according to our agreement in this matter, is not to be used for any other purpose, including as evidence in this case. If this does not accord with your understanding, please contact me immediately.

The letter follows up on your email on October 14, 2008 that contained your proposed protocol for the inspection of Internet servers at our clients' facilities. We have numerous concerns with this proposed protocol and find it insufficient for a number of reasons.

Compliance with the Court's August 7, 2008 Order

As we have noted to you in our previous letters sent on September 5, 2008, September 19, 2008, September 26, 2008 and October 13, 2008, we have made it clear that our clients provide unmanaged Internet hosting, and that, pursuant to their service agreements with their customers, our clients are not authorized, nor are they able to, access their clients' password-

EXHIBIT
A
ALL-STATE® INTERNATIONAL

protected content. Our primary question about this upcoming server inspection was how your client would propose to conduct the inspection, without the passwords necessary to access the servers, in a way that limits the inspection to "publically available information" "without accessing password protected contents" in full compliance with the Court's Aug 7, 2008 Order, which provides:

> Defendants are not required to disclose private information stored on their computers, they are only required to disclose **information that the third-parties have made available to the public.**[1]
>
> [T]he discovery is **limited to publically available contents.** Defendants have offered no evidence to suggest that they cannot produce **publically available contents without accessing password protected contents.**[2]

Nowhere in your proposed protocol do you discuss *how* you intend to perform the server inspection in compliance with the Court's order. You merely say that "Guidance Software will comply with the Court's order and referenced Exhibits" without any further discussion as to what steps, in particular, your forensic examiner will take to ensure compliance with the Court's order.

This lack of explanation is completely unacceptable and insufficient in light of the Court's order. Please provide us with a protocol for this inspection that includes *detailed* steps that your expert will take to comply with the Court's order. The entire point of developing an agreed protocol is to establish exactly how the inspection will be performed. We frankly do not understand how your forensic consultant intends to proceed without violating the privacy rights of the third parties and potentially violating federal statutes. We have been asking this question from the beginning and neither you, Mr. Coombs, nor your consultant have been able to give us an answer. Your comments on October 14, 2008 essentially dodge that critical question again and suggest "trust us." This is unacceptable. We need to know the technical details before we can agree to your protocol.

Proposed Notice to Customers

We also object to the two proposed notice requirements set forth in your proposed protocol.

Our clients believe its customers should have notice 24 hours prior to the server interruption instead of the 12 hours notice that you propose. While our clients have sent their customers 12 hour "takedown" notices in the past, this server interruption requires a much more

[1] Court's Aug 7, 2008 Order 2:23-25
[2] Court's Aug 7, 2008 Order 3:5-7

complicated response. 12 hours notice may be sufficient to take down certain material from a website, but it is not enough time to devise entire contingency plans for a service interruption.

Also, many of our clients' customers are in China, and the time difference between our clients' time zone and their customers' time zone makes it such that 12 hours may not be sufficient time to allow them to plan for contingencies for a server interruption. For instance, sending a China-based customer a notice at 8:00 p.m. local time (after business hours) and initiating the server inspection at 8:00 a.m. local time would likely prevent customers from being able to prepare adequately for the service interruption.

We also find the following portion of your proposed protocol to be objectionable:

> Defendants may not "tipoff" or otherwise suggest to their "customers" the purpose of the inspection other than to state after LV has provided notice identifying a specific server, that "service may be disrupted on [a specified date]" as to the identified server only.

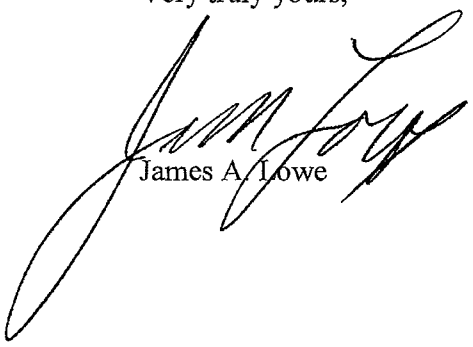
While our clients understand that you would prefer that the service disruption notices not refer to this upcoming inspection, placing such a restriction on our clients' notices to their customers will negatively affect their business relationships, which are directly tied to their ability to offer uninterrupted Internet hosting services. In order to maintain their reputation as providers of quality Internet hosting services, our clients seek to prevent any disruptions of service to their customers, and if any such disruptions are necessary, to sufficiently explain the bases for these disruptions to assuage any of their customers' concerns as to the quality of our clients' services. There has never been such a server interruption as you are proposing and it will shock customers.

The negative ramifications of a "generic" disruption notice to our clients' business reputation would outweigh any potential benefits. While you may believe that a "generic" service interruption notice will prevent any website operator from removing potentially offending content, this may not be the case. Our clients almost never send server interruption notices and, in the rare times when they do, they explain the reasons for the interruption. A "generic" interruption notice with no explanation would likely cause confusion, possibly causing website operators to speculate as to the cause of the interruption. This speculation would not only harm our clients' business reputation, it would likely cause any potentially offending website operators to remove content anyway. We must agree on some notice that is reasonable on its face and that will not panic customers.

Please advise us as to how you plan to revise your proposed protocol to address these issues. We are especially concerned about your complete failure to explain how your forensic expert will comply with the Court's August 7, 2008 order. Preventing the disclosure of

password-protected content is of paramount importance to our clients, and the Court's order acknowledges the significance of preventing such disclosure.

Very truly yours,



James A. Lowe

JAL:pam

cc: Clients (via email)

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

Louis Vuitton Malletier, S.A.,

Plaintiff,

v.

Akanoc Solutions, Inc., et al.,

Defendants.

_____/

NO. C 07-03952 JW

ORDER OVERRULING DEFENDANTS' OBJECTION TO THE MAGISTRATE JUDGE'S ORDER COMPELLING PRODUCTION OF DOCUMENTS

I. INTRODUCTION

Luis Vuitton Malletier, S.A. ("Plaintiff") brings this action against Akonoc Solutions, Managed Solutions Group, and Steven Chen (collectively, "Defendants"), alleging contributory and vicarious trademark and copyright infringement. Defendants are internet service providers who host third-party websites on their servers. Plaintiff alleges that Defendants have knowingly facilitated the sale of counterfeit products through their hosting of web sites that sell such goods. (See Amended Complaint for Contributory and Vicarious Trademark Infringement, Docket Item No. 71.)

A discovery dispute arose concerning Plaintiff's request for information stored on Defendants' servers. On July 15, 2008, Magistrate Judge Lloyd granted Plaintiff's motion to compel. (hereafter, "Order to Compel," Docket Item No. 65.) Judge Lloyd ordered Defendants to "produce all responsive publicly posted Internet content evidencing offers made of counterfeit Louis Vuitton merchandise and traffic logs evidencing the volume of underlying counterfeit activity....The discovery shall be limited to the 67 allegedly infringing websites identified by plaintiff." (Id. at 5.)

Presently before the Court is Defendants' objection to the order to compel. (hereafter, "Objection," Docket Item No. 69.)

II. DISCUSSION

Defendants object to the order on the grounds that: (1) disclosing information stored by third-parties would violate the Stored Communications Act ("SCA") 18, U.S.C. § 2702; and (2) producing the contents requested is impossible. (Objection at 1, 9.)

A district court reviews a magistrate judge's ruling under the "clearly erroneous" or "contrary to law" standard. 28 U.S.C. § 636(b)(1)(A); Fed. R. Civ. P. 72(a); Bahn v. NME Hospitals, Inc., 929 F.2d 1404, 1414 (9th Cir. 1991).

The Court considers each issue in turn.

A. Stored Communications Act

Defendants contend that Judge Lloyd erred by ordering discovery that would require them to violate the SCA. (Objection at 1.)

The SCA "prevents 'providers' of communication services from divulging private communication to certain entities and/or individuals." Quon v. Arch Wireless Operating Co., —F.3d—, 2008 WL 2440559 at *5 (9th Cir., June 18, 2008). However, the SCA does not "criminalize or create civil liability for acts of individuals who 'intercept' or 'access' communications that are otherwise readily accessible by the general public." Snow v. Directv, Inc., 450 F.3d 1314, 1320-21 (11th Cir. 2006).

Defendants contend that the discovery sought violates the SCA because it requires them to disclose private information belonging to third-parties. (Objection at 3.) Defendants' contention blatantly misrepresents Judge Lloyd's order. Judge Lloyd specifically limited his order to all "publicly posted Internet content." (Order to Compel at 5.) Defendants are not required to disclose private information stored on their computers; they are only required to disclose information that the third-parties have made available to the public. Accordingly, the Court finds that the Order to Compel does not violate the SCA.

B. Compliance

Defendants contend that they cannot comply with the Order to Compel because (1) they do not have access to the password protected content and (2) they have approximately 1500 servers, which make any search unduly burdensome. (Objection at 9.)

First, as discussed above, the discovery is limited to publicly available contents. Defendants have offered no evidence to suggest that they cannot produce publicly available contents without accessing password protected contents. Second, although Defendants claim they have more than 1500 servers, discovery is limited to 67 specific web sites. (Order to Compel at 5.) Defendants have offered no evidence to suggest that they cannot narrow the number of servers on which responsive contents might exist based on these 67 specific web sites and their own business records. Accordingly, the Court finds Defendants have not shown that the discovery sought is unduly burdensome.

III. CONCLUSION

The Court OVERRULES Defendants' objection to the Order to Compel. As directed by Judge Lloyd, the parties shall meet and confer to determine an appropriate protocol for obtaining the discovery at issue. All other discovery disputes are referred to Judge Lloyd.

Dated: August 7, 2008

JAMES WARE
United States District Judge

THIS IS TO CERTIFY THAT COPIES OF THIS ORDER HAVE BEEN DELIVERED TO:

Annie S Wang annie@coombspc.com
Brian S. Edwards bse@gauntlettlaw.com
David A. Gauntlett info@gauntlettlaw.com
J. Andrew Coombs andy@coombspc.com
James A. Lowe info@gauntlettlaw.com

Dated: August 7, 2008

Richard W. Wieking, Clerk

By: /s/ JW Chambers
Elizabeth Garcia
Courtroom Deputy

EXHIBIT C

GAUNTLETT & ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

August 8, 2008

VIA E-MAIL
andy@coombspc.com

J. Andrew Coombs, Esq.
Annie S. Wang, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.*
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

- **Attempted Compliance with District Court's Order**

Dear Mr. Coombs:

In advance of our phone conference on August 14, 2008, we would appreciate an explanation or your suggestions as to how Akanoc and Managed Solutions Group can comply with the District Court's order concerning the "publicly accessible files" on their servers.

As we have repeatedly told you, the Defendants only provide unmanaged hosting services, meaning their customers are the only ones that know the passwords required to access their files. This is not a matter of the Defendants' reluctance to access these files. The Defendants actually cannot access the files because they do not have the passwords necessary to do so.

We look forward to hearing about any techniques or protocols that Louis Vuitton proposes to employ in order to circumvent this password protection and to access only "publicly accessible files."

Very truly yours,

James A. Lowe

JAL:pam
cc: Clients (via email)
10562-002-8/8/2008-162447.1

EXHIBIT
C
ALL-STATE® INTERNATIONAL

EXHIBIT D

GAUNTLETT & ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

September 5, 2008

CONFIDENTIAL SETTLEMENT COMMUNICATION

This communication constitutes an offer of compromise and is subject to the provisions of California Evidence Code § 1152, Rule 408 of the Federal Rules of Evidence and all other similar rules.

VIA E-MAIL
annie@coombspc.com

Annie Wang, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: ***Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.***
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

- **List of Server Information Related to Complaint Websites**

Dear Ms. Wang:

In furtherance of our effort to agree with Louis Vuitton to a protocol for inspection of Internet servers at our clients' facilities, we provide the following information for use by your forensic computer consultant and your office to identify potential servers to inspect and to develop a practical protocol. This information, according to our agreement in this matter, is not to be used for any other purpose, including as evidence in this case. If this does not accord with your understanding, please contact me immediately.

In compliance with Judge Ware's Order of August 7, 2008 our clients have searched their business records and physical plant to identify servers potentially associated with the 67 websites identified by Louis Vuitton. The attached list identifies the "extra" Internet Protocol ("IP") addresses about which your office has complained allegedly associated with various Internet domain names, the main "server" IP addresses associated with the identified IP addresses, the server location, the server operating system, and the server status for the servers related to domains named in the First Amended Complaint. Domains named in the First Amended Complaint that are not on this list are those that Defendants found to be either outside their assigned IP range or non-functional. In any case our clients were unable to identify any server with those domain names listed in the First Amended Complaint but not listed on the attached

EXHIBIT
D
ALL-STATE® INTERNATIONAL

chart. Because there is no record of these domains being hosted on IP addresses within Defendants' range, Defendants have no server information related to these domains.

The Defendants' process for compiling this list involved the following steps: **First**, the Defendants referred back to the records that they compiled at the time of the complaint in order to determine the "extra" IP that the domain was allegedly using at the time. **Second**, the Defendants searched through internal emails (the same emails provided to you yesterday on a CD-ROM) in order to tie the "extra" IP to a main "server" IP address. It has been our clients' general practice for some time to use an internal email to record the IP addresses assigned to particular "main IP addresses." **Third**, the Defendants identified the physical location of the servers by referencing the CPRO database, which ties a server's main IP address to physical servers and their respective locations. **Fourth**, the Defendants confirmed what operating system each server was running, and whether the server was online.

Under the "Rack/Slot Location" column of the attached list, the locations are listed in a format that reads, for example, "C36B-H12." The first number after the letter C is the rack number where the server is located. The letter following this number (either A or B) indicates on what shelf the server is located; A is the top shelf of the rack, B is the bottom shelf of the rack. The number following the H is the slot number where the server is located. This means that a server location "C36B-H12" means that the server is located on the bottom shelf of rack 36 in slot 12. Defendants have confirmed that the racks and slot numbers are openly labeled and easily identifiable.

The Defendants exerted extensive efforts to compile this list, but were unable to locate the main "server" IP information for five of the extra IP addresses. Without this information, the Defendants were unable to locate the physical server possibly used in connection with the extra IP addresses, as well as any information about the server itself, such as operating system and current status. The Defendants have determined that these five "unidentified" extra IP addresses are assigned (or were perhaps reassigned) to customers providing only Voice Over IP Service (VoIP) services that to our clients' knowledge are not used for any Websites.

So of the IP addresses you originally identified (alleged to be associated with accused domain names), our clients were never able to identify more than 30 operational addresses that were within their assigned IP ranges. Of those, our clients have been able to tie the "extra" IP addresses to 25 main IP addresses and only 20 servers (out of approximately 1,500 servers). Five sets of two each of the "extra" IP addresses appear to be on the same server.

Finally, in response to your question posed during our conference call last week, Defendants have verified that all of the default passwords on the listed servers have been changed by the users, meaning that the default passwords will not provide access to the server contents. Our clients have no passwords and have no access to the servers' operating systems. As we have explained previously, access would have to be made by requesting the customers to allow access (and if our clients are asked to request that their customers give them access, please tell us what you propose we use as an explanation for the customers because our clients do not ordinarily ever ask for such access and the customers will certainly demand an explanation).

Perhaps your computer consultant has some technique for hacking into the systems to obtain access although that would appear to be contrary to the Court's order of August 7.

We remain concerned about how you intend to limit the server inspection to "publically available information" "without accessing password protected contents" as the District Court has limited the inspection.[1] We have repeatedly explained that our clients have no way of doing this and we have yet to understand how your forensic consultant intends to do it. This will need to be addressed in any protocol to avoid violation of the Stored Communications Act. During our recent telephone discussion it sounded as if your consultant perhaps intended to take a complete image of hard drives and then examine the entire password protected hard drive, bypassing the password protection of our clients' customers, using keyword searches to identify potentially interesting data. But I did not understand that he had any way of limiting any search to "publically available information" "without accessing password protected contents." Please explain how your proposed protocol will comply with Judge Ware's order. We look forward to hearing from you about your proposed protocol.

Very truly yours,

James A. Lowe

JAL:pam
Enclosure: Server listing
cc: Clients (via email)

[1] Aug 7, 2008 Order, 2:23-25 ("Defendants are not required to disclose private information stored on their computers, they are only required to disclose **information that the third-parties have made available to the public.**"); 3:5-7 ("[T]he discovery is **limited to publically available contents.** Defendants have offered no evidence to suggest that they cannot produce **publically available contents without accessing password protected contents.**")

Domain Name	Extra IP	Main IP	Operating System	Rack/Slot Location	Online/Offline
1/14/08 Noticed Sites					
bag4sell.com	204.16.196.218	Cannot Identify IP			
bigworldshoes.com	204.16.193.49	205.209.161.147	Win Server 03 STD	C36B-H12	Online
brandfashioner.com	204.16.195.58	204.13.69.61	Win Server 03 STD	C38B-H14	Online
buymyshoes.net	205.209.171.44	205.209.136.90	Win Server 03 STD	C50A-H06	Online
dreamyshoes.com	204.16.198.150	204.13.69.170	Win Server 03 STD	C42A-H01	Online
eastarbiz.com	205.209.140.66	205.209.140.66	Win Server 03 STD	C33B-H16	Online
famous-shop.com	205.209.143.93	205.209.143.93	Win Server 03 Web edition	C44A-H09	Online
handbagsell.com	205.209.185.74	Cannot Identify IP			
innike.com	205.209.165.82	205.209.142.3	Win Server 03 STD	C46A-H02	Online
louisvuittonbagz.com	66.79.176.207	66.79.168.170	FedoraCore 3	C29A-H01	Online
luxury2us.com	204.16.193.105	204.13.69.210	Win Server 03 STD	C42B-H01	Online
lvbagz.com	66.79.176.207	66.79.168.170	FedoraCore 3	C29A-H01	Online
nikeshoesoffer.com	205.209.175.218	204.13.69.10	Win Server 03 Web edition	C38A-H06	Online
nikewto.com	205.209.168.3	205.209.142.235	Win Server 03 STD	C48B-H17	Online
pickyourorder.com	205.209.185.114	205.209.143.27	Win Server 03 Web edition	C43A-H17	Online
replica-ebags.com	204.16.193.146	Cannot Identify IP			
shoes-order.com	204.13.66.161	204.13.69.210	Win Server 03 Web edition	C42B-H01	Online
soapparel.com	204.16.192.244	205.209.136.92	FedoraCore 4	C50A-H08	Online
tytrade88.com	205.209.136.83	205.209.136.83	Win Server 03 Web edition	C50A-H02	Online
wearonline.net	204.13.70.133	204.13.69.170	Win Server 03 STD	C42A-H01	Online
3/31/08 Noticed Sites					
soapparel.net	204.13.71.8	204.13.69.92	CentOS4.3	C39A-H08	Online
6/2/08 Noticed Sites					
att88.com	66.79.177.228	Cannot Identify IP			
lkkfashion2006.com	204.16.192.200	205.209.136.84	Win Server 03 Web edition	C50A-H03	Online
lv-handbag.com	204.16.193.105	204.13.69.210	Win Server 03 Web edition	C42B-H01	Online
replicabe.com	205.209.148.1	205.209.143.44	FreeBSD 5.4	C43B-H03	Online
top-handbag.com	205.209.155.48	205.209.136.90	Win Server 03 STD	C50A-H06	Online
bag1881.net	205.209.175.160	204.13.69.10	Win Server 03 Web edition	C38A-H06	Online
queen-bag.com	66.79.177.229	Cannot Identify IP			
6/20/2008 Noticed Sites					
sportsvendor.biz	208.77.45.140	208.77.45.140	Win Server 03 STD	C101B-H08	Online
6/24/08 Noticed sites					
brandstreets.com.cn	205.209.184.220	205.209.161.20	Win Server 03 Web edition	C35A-H13	Online

EXHIBIT E

GAUNTLETT &
ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

September 19, 2008

CONFIDENTIAL SETTLEMENT COMMUNICATION

This communication constitutes an offer of compromise and is subject to the provisions of California Evidence Code § 1152, Rule 408 of the Federal Rules of Evidence and all other similar rules.

VIA E-MAIL
annie@coombspc.com

Annie Wang, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: ***Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.***
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

- **Request for Server Inspection Protocol**

Dear Ms. Wang:

In furtherance of our effort to agree with Louis Vuitton to a protocol for inspection of Internet servers at our clients' facilities, as required by Judge Ware's Order of August 7, 2008, we provide the following information for use by your forensic computer consultant and your office to identify potential servers to inspect and to develop a practical protocol. This information, according to our agreement in this matter, is not to be used for any other purpose, including as evidence in this case. If this does not accord with your understanding, please contact me immediately.

On September 5, 2008, we sent you a list identifying the (1) "extra" Internet Protocol ("IP") addresses about which your office has complained allegedly associated with various Internet domain names, (2) the main "server" IP addresses associated with the identified IP addresses, (3) the server location, (4) the server operating system, and (5) the server status for the servers related to 67 domains named in the First Amended Complaint. Our letter also confirmed that, in response to a question you posed earlier, Defendants have verified that all of the default passwords on the listed servers have been changed by the users, meaning that the default passwords will not provide access to the server contents.

We have now complied with all of your information requests in preparation for the server inspection. To date, however, we have not received from you a proposed protocol for performing the server inspection. Without the passwords necessary to access the servers, we need to understand how you propose to conduct the inspection in a way that limits the inspection to "publically available information" "without accessing password protected contents" as set forth in the District Court's order.[1]

We have asked you during telephone conferences and in previous letters to propose a protocol for this inspection but have received no proposal to date. We look forward to hearing from you about your proposed protocol.

Very truly yours,

James A. Lowe

JAL:pam
Enclosure:
cc: Clients (via email)

[1] Aug 7, 2008 Order, 2:23-25 ("Defendants are not required to disclose private information stored on their computers, they are only required to disclose **information that the third-parties have made available to the public.**"); 3:5-7 ("[T]he discovery is **limited to publically available contents.** Defendants have offered no evidence to suggest that they cannot produce **publically available contents without accessing password protected contents.**")

EXHIBIT F

GAUNTLETT & ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

September 26, 2008

CONFIDENTIAL SETTLEMENT COMMUNICATION

This communication constitutes an offer of compromise and is subject to the provisions of California Evidence Code § 1152, Rule 408 of the Federal Rules of Evidence and all other similar rules.

VIA E-MAIL
annie@coombspc.com

Annie Wang, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: ***Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.***
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

- **Request for Server Inspection Protocol**

Dear Ms. Wang:

In furtherance of our effort to agree with Louis Vuitton to a protocol for inspection of Internet servers at our clients' facilities, as required by Judge Ware's Order of August 7, 2008, we provide the following information for use by your forensic computer consultant and your office to identify potential servers to inspect and to develop a practical protocol. This information, according to our agreement in this matter, is not to be used for any other purpose, including as evidence in this case. If this does not accord with your understanding, please contact me immediately.

This letter follows up on our letters sent to you on September 5, 2008 and September 19, 2008.

On September 5, 2008, we sent you a list identifying the (1) "extra" Internet Protocol ("IP") addresses about which your office has complained allegedly associated with various Internet domain names, (2) the main "server" IP addresses associated with the identified IP addresses, (3) the server location, (4) the server operating system, and (5) the server status for the servers related to 67 domains named in the First Amended Complaint. Our letter also confirmed that, in response to a question you posed earlier, Defendants have verified that all of the default

passwords on the listed servers have been changed by the users, meaning that the default passwords will not provide access to the server contents.

On September 19, 2008, we sent you a letter confirming our compliance with all of your information requests and requesting from you a proposed protocol for performing the server inspection.

As we have indicated, our clients do not have the passwords necessary to access the servers. We need to understand how you propose to conduct the inspection, without these passwords, in a way that limits the inspection to "publically available information" "without accessing password protected contents" as set forth in the District Court's order.[1]

Despite our prior requests for you to propose a protocol for this inspection, we have received no proposal to date. We look forward to hearing from you about your proposed protocol.

Very truly yours,

Christopher Lai

CL:arm

cc: Clients (via email)
James A. Lowe

[1] Aug 7, 2008 Order, 2:23-25 ("Defendants are not required to disclose private information stored on their computers, they are only required to disclose **information that the third-parties have made available to the public.**"); 3:5-7 ("[T]he discovery is **limited to publically available contents.** Defendants have offered no evidence to suggest that they cannot produce **publically available contents without accessing password protected contents.**")

EXHIBIT G

GAUNTLETT & ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

October 13, 2008

CONFIDENTIAL SETTLEMENT COMMUNICATION

This communication constitutes an offer of compromise and is subject to the provisions of California Evidence Code § 1152, Rule 408 of the Federal Rules of Evidence and all other similar rules.

VIA E-MAIL
annie@coombspc.com

Annie Wang, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.*
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

- **Request for Server Inspection Protocol**

Dear Ms. Wang:

In furtherance of our effort to agree with Louis Vuitton to a protocol for inspection of Internet servers at our clients' facilities, as required by Judge Ware's Order of August 7, 2008, we provide the following information for use by your forensic computer consultant and your office to identify potential servers to inspect and to develop a practical protocol. This information, according to our agreement in this matter, is not to be used for any other purpose, including as evidence in this case. If this does not accord with your understanding, please contact me immediately.

This letter follows up on our letters sent to you on September 5, 2008, September 19, 2008 and September 26, 2008.

On September 5, 2008, we sent you a list identifying the (1) "extra" Internet Protocol ("IP") addresses about which your office has complained allegedly associated with various Internet domain names, (2) the main "server" IP addresses associated with the identified IP addresses, (3) the server location, (4) the server operating system, and (5) the server status for the servers related to 67 domains named in the First Amended Complaint. Our letter also confirmed that, in response to a question you posed earlier, Defendants have verified that all of the default

passwords on the listed servers have been changed by the users, meaning that the default passwords will not provide access to the server contents.

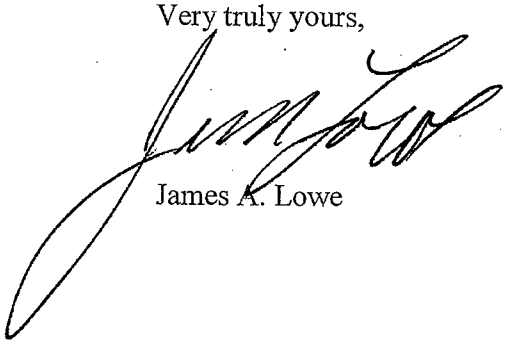
On September 19, 2008, we sent you a letter confirming our compliance with all of your information requests and requesting from you a proposed protocol for performing the server inspection.

On September 26, 2008, we sent you a letter once again confirming our compliance and requesting a proposed protocol from you. In response, you sent us an email that same day confirming that you and your client were "exploring some alternatives" and would advise us about a final protocol "as soon as possible."

We have received no proposal to date and no follow up to your September 26. 2008 email. As we have indicated, our clients do not have the passwords necessary to access the servers. We need to understand how you propose to conduct the inspection, without these passwords, in a way that limits the inspection to "publically available information" "without accessing password protected contents" as set forth in the District Court's order.[1]

We look forward to hearing from you about your proposed protocol.

Very truly yours,



James A. Lowe

JAL:pam

cc: Clients (via email)

[1] Aug 7, 2008 Order, 2:23-25 ("Defendants are not required to disclose private information stored on their computers, they are only required to disclose **information that the third-parties have made available to the** public."); 3:5-7 ("[T]he discovery is **limited to publically available contents.** Defendants have offered no evidence to suggest that they cannot produce **publically available contents without accessing password protected contents.**")

EXHIBIT H

GAUNTLETT & ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

August 22, 2008

VIA E-MAIL
andy@coombspc.com

J. Andrew Coombs, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: ***Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.***
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

- **Proof of Expenses Incurred by Vuitton's Rule 30(b)(6) Witness**

Dear Mr. Coombs:

Your proposed Preliminary Pretrial and Trial Setting Conference Statement stated that Defendants have not paid one-half of the actual, reasonable out-of-pocket expenses incurred by Vuitton during the deposition of its Rule 30(b)(6) witness. This is unpaid because you have not yet provided us with any actual evidence (i.e. actual bills) of the travel expenses incurred.

We must have the billing documentation in order to submit it to our clients insurer with a request for payment. When you provide evidence of the travel expenses to us, we can evaluate reasonableness and submit them for payment.

Very truly yours,

James A. Lowe

JAL:pam
cc: Clients (via email)

EXHIBIT
H
ALL-STATE® INTERNATIONAL

10562-002-8/22/2008-162598.1

EXHIBIT I

GAUNTLETT &
ASSOCIATES
ATTORNEYS AT LAW

18400 Von Karman, Suite 300
Irvine, California 92612
Phone: (949) 553-1010
Facsimile: (949) 553-2050

Email: info@gauntlettlaw.com
Website: www.gauntlettlaw.com

Our File Number:
10562-002

November 12, 2008.

VIA E-MAIL and U.S. MAIL
andy@coombspc.com

J. Andrew Coombs, Esq.
LAW OFFICES J. ANDREW COOMBS, APC
517 E. Wilson Avenue, Suite 202
Glendale, CA 91206-5902

Re: *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al.*
U.S.D.C., Northern District of CA, Case No. C07 3952-JW

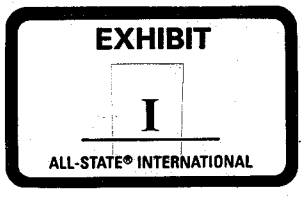
- **A Proposal For Server Inspection**

Dear Mr. Coombs:

We have previously provided you a list of and details about Internet servers that may have been used by the Websites that Louis Vuitton has accused of infringing its copyrights and trademarks. As we have informed you, all the servers are password protected by our clients' customers. Our clients do not have any ability to access the contents of the hard drives without obtaining passwords from their customers (something they have never done) and you have told us that the passwords should not be requested from customers because third parties might then be alerted to remove material from the servers that you want to inspect.

While you have alleged that there are Websites publically accessible through an Internet browser (like Google), our clients have no way of accessing such Websites through the servers (even if they might be using our clients' servers to store data that a Website displays on Google and even if our clients had passwords to access those servers—they don't). This is because there is no way to access Website data directly through access to a hard drive.

It is absolutely necessary, to our knowledge, to use an Internet browser accessing an Internet address to cause the Website to be displayed and causing the Website to use its own programming (HTML) to call up the pages of information that are intended to be displayed by the Website. We expect that operators of Websites will have some data that is intended to be publically displayed by a Website and some data (such as logs, sales information, customer information, banking information, etc.) that is stored but intended only for the private use of the



Website operator. We simply know of no technical method of indirectly accessing Website data, or even of identifying what data goes with what Website.

The servers potentially used by accused Websites also store data for other of the defendants' customers for assorted non-website purposes. So it is important to avoid accessing such private data.

We have attempted to work with you to develop a protocol for inspection of the defendants' Internet servers that will comply with the Magistrate Judge's order as interpreted by the District Judge. We have repeatedly asked your office and your forensic consultant how you propose to inspect the server contents while avoiding access to non-public materials as required by Judge Ware's August 7, 2008 order.

But you have not proposed any way of looking at "publically available" server content without also accessing private content of third parties. You have only said it will be done. But how? Our clients have no idea how to accomplish this task. We have contacted numerous computer forensic organizations and experts trying to determine how this might be done. But we have found no one who can tell us how to accomplish the goal of the orders.

So we want your thoughts about a method that might be appropriate under the law. We want to suggest consideration of a protocol including the following steps:

(1) A forensic examiner, at Louis Vuitton's expense, would copy the data on the relevant server hard drives and then use software to search for and extract data from the copied hard drive that appears to be data for a public Website that references Louis Vuitton products. This process would be performed **without** discussing or disclosing the search results with either party or their counsel.

(2) The forensic examiner will then submit such evidence that he thinks meets the above test together with an explanation of search methods utilized, directly to the Magistrate Judge for an in-camera review **without** providing it to either party.

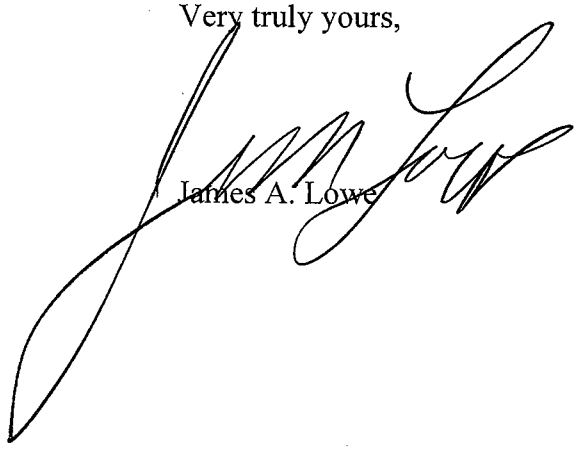
(3) The Magistrate Judge would review the data from the forensic examiner and if he can identify any relevant information, within the scope of Judge Ware's August 7, 2008 order, from publically available and not private portions of the server hard drives, he would provide that limited information to counsel for the parties to review.

(4) The parties could thereafter agree or challenge the adequacy or relevance of the information provided.

As we have indicated to you previously, we do not know how to conduct a search in such a way as to limit the results to "publically available" content in compliance with the Court's August 7, 2008 order. We feel that this proposal may serve both parties because it circumvents the parties' disagreements on what constitutes "publically available" content while allowing this server inspection process to move forward.

We look forward to your response to our proposal.

Very truly yours,



James A. Lowe

JAL:pam
cc: Clients (via email)