

1 **Jason K. Singleton, State Bar #166170**
jason@singletonlawgroup.com
2 **Richard E. Grabowski, State Bar #236207**
rgrabowski@mckinleyville.net
3 **SINGLETON LAW GROUP**
611 "L" Street, Suite A
4 **Eureka, CA 95501**
(707) 441-1177
5 **FAX 441-1533**

6 **Attorneys for Plaintiff, ASIS Internet Services**

7 **UNITED STATES DISTRICT COURT**
8 **NORTHERN DISTRICT OF CALIFORNIA**

9 **ASIS INTERNET SERVICES, a California**)
10 **corporation,**)

11 **Plaintiff,**)
12 **vs.**)

13 **OPTIN GLOBAL, INC., a Delaware**)
14 **Corporation, also dba Vision Media Limited**)
15 **Corp., USA Lenders Network, USA Lenders,**)
16 **and USA Debt Consolidation Service; et al.,**)

17 **Defendants.**)

Case No. C-05-5124 JCS

**MOTION FOR SUMMARY ADJUDICATION
OF ISSUES; MEMORANDUM OF POINTS
AND AUTHORITIES IN SUPPORT OF
MOTION**

DATE: March 14, 2008

TIME: 1:30 p.m.

CTRM: 15, 18TH FLOOR

TABLE OF CONTENTS

1

2 I. MEMORANDUM OF POINTS AND AUTHORITIES..... 1

3 A. STATEMENT OF FACTS..... 1

4 1. History 1

5 2. Plaintiff is an Internet Access Provider (hereafter IAP) and Email Service
6 Provider (hereafter ESP) 6

7 3. The emails at issue were sent to ASIS email accounts and that they were
8 received by ASIS..... 7

9 4. The subject emails contain false header information..... 7

10 5. The subject emails contain false or misleading subject lines..... 10

11 6. The subject emails do not contain a valid unsubscribe option and a physical
12 opt-out address. 11

13 7. The emails at issue were not solicited by the intended recipients..... 11

14 B. ARGUMENT 11

15 1. Summary adjudication of issues and defenses is within the authority of the Court. 11

16 2. Standard for Summary Judgment. 12

17 3. There is no factual or legal basis for the defense asserted by Defendant that
18 Plaintiff assumed the risk 12

19 4. There is no factual or legal basis for the defense asserted by Defendant that
20 any loss incurred by Plaintiff was proximately caused by the acts of third
21 parties or non-parties. 14

22 5. There is no factual or legal basis for the defense asserted by Defendant that
23 Plaintiff’s claims are barred by the doctrine of unclean hands 16

24 6. There is no factual or legal basis for the defense asserted by Defendant that
25 Plaintiff has failed to mitigate damages, if any..... 17

26 7. There is no factual or legal basis for the defense asserted by Defendant that
27 damages, if any, were proximately caused by Plaintiff..... 18

28 8. There is no factual or legal basis for the defense asserted by Defendant that
Plaintiff invited and consented to the acts of Defendant. There is no factual
dispute that the emails were not solicited by the intended recipients. 19

9. There is no factual or legal basis for the defense asserted by Defendant that
Plaintiff waived any claim or cause of action against Defendant 20

10. There is no factual or legal basis for the defense asserted by Defendant that
Plaintiff’s claims are barred under the doctrine of preemption..... 20

11. There is no factual dispute that Plaintiff is a provider of Internet Access as
defined in 15 *USC* 7706(g)(1). There is no factual dispute that Plaintiff is a
provider of Email Services within the definition of *California Business and
Professions Code* §17529.5 .. 21

12. There is no factual dispute that the emails at issue were sent or transmitted to
ASIS email accounts and that they were received by ASIS.. 22

13. There is no factual dispute that the subject emails contain false header
information 22

14. There is no factual dispute that the emails contain false or misleading subject
lines ... 23

15. There is no factual dispute that the emails do not contain a valid unsubscribe
option and a physical opt-out address in violation of 15 *USC* 7704(a)(5).... 24

III. CONCLUSION 25

TABLE OF AUTHORITIES

CASES

Alber v. Owens, 66 Cal.2d 790 at 799 (Cal. 1967)..... 13

Anderson v. Liberty Lobby, Inc., 477 U.S. 242 at 248 and 249 (1986) 12

Barker v. Norman, 651 F.2d 1107 at 1123 (5th Cir., 1981)..... 12

Beeman v. Burling, 216 Cal.App.3d 1586 at 1589 (Cal.App. 1 Dist.,1990)..... 18

Crane v. Cedar Rapids & I. C. Ry. Co., 395 U.S. 164 at 166 (1969) 13

Dollar Systems, Inc., v Avcar Leasing Systems, Inc., 890 F.2nd 165, 173 (9th Cir. 1989) 16

Engine Mfrs. Ass'n v. South Coast Air Quality Management Dist., 498 F.3d 1031 at 1039
(9th Cir., 2007)..... 21

Jones v. R.R. Donnelley & Sons Co., 541 U.S. 369, 369 (2004)..... 20

Knight v. Jewett, 3 Cal.4th 296, 308 (Cal. 1992) 13

Moothart v. Bell, 21 F.3d 1499, 1506-07 (10th Cir.1994)..... 18

Nintendo v. Dragon Pacific International, 40 F.3d 1007, 1011 (9th Cir.1994) 18

Palsgraf v. Long Island Railroad Co., 248 N.Y. 339, 162 N.E. 99 (1928) 18

Turnbull & Turnbull v. ARA Transportation, Inc., 219 Cal.App.3d 811 at 826, 268 Cal.Rptr. 856
(Cal.App.3.Dist.,1990)..... 18

Wang Laboratories, Inc. v. Mitsubishi Electronics, America, Inc., 860 F.Supp. 1448, 1450
(CD CA 1993) 12

Williams v. Sinclair, 529 F2d 1383 at (9th Cir. 1975) 12

STATUTES

15 USC 45 24

15 USC 7701 13

15 USC 7702(12) 14

15 USC 7702(17) 19

15 USC 7702(9) 14

15 USC 7703 17

15 USC 7704 14, 17

15 USC 7704 (a)(1)(A) and (b)(3) 23

15 USC 7704(a) 19, 22

15 USC 7704(a)(1)–(5) 22

15 USC 7704(a)(1)(C) 23

15 USC 7704(a)(4)..... 19

15 USC 7704(a)(5)(A)(ii) 24

15 USC 7704(a)(5)(A)(iii) 11, 24

15 USC 7704(a)(6)..... 23

15 USC 7706 14, 17

15 USC 7706(g) 22

15 USC 7706(g)(2)..... 15

15 USC 7706(g)(3)(D) 14

15 USC 7707(b)(1)..... 21

15 USC 7707(b)(2)(B) 21

18 USC 1030(e)(2)(B)..... 22

28 USC 1658(a) 20

47 USC 231(e)(4) 21

California Business and Professions Code §17529.1(h) 21

California Business and Professions Code §17529.5passim

1	<i>California Code of Civil Procedure</i> §338	20
	<i>California Code of Civil Procedure</i> §340(a)	20
2	<i>CAN SPAM Act of 2003</i>	passim
3	<u>OTHER AUTHORITIES</u>	
4	SENATE REPORT NO. 108-102, 2004 U.S.C.C.A.N. 2348, July 16, 2003	16, 17
5	<u>RULES</u>	
6	<i>FRCP</i> Rule 56(a).....	12
7	<i>FRCP</i> Rule 56(a)(c) and (d)	12
8	<i>FRCP</i> Rule 56(c)	12
9	<i>FRCP</i> Rule 56(d).....	12
10	<u>CONSTITUTIONAL PROVISIONS</u>	
11	<i>U.S. Const.</i> Art. 6, cl. 2	20
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 I. MEMORANDUM OF POINTS AND AUTHORITIES

2 A. STATEMENT OF FACTS

3 1. History

4 At Azoogle's inception, around 2001, Azoogle was entirely an email company. That is, its entire
5 marketing model was via bulk commercial email. See Exhibit A to the Declaration of Richard
6 Grabowski (hereinafter RG), Don Mathis P111, submitted under seal. By August 2004 Azoogle was a
7 \$50 million a year company. See Exhibit B to RG, Joe Speiser Depo., P35-36, and Exhibit 3 (Bate No.
8 0853).

9 Azoogle itself admitted in correspondence with Spamhaus that it's (Azoogle's) "past history has
10 not been great". (AZ-SP 043, Exhibit C to RG, submitted under seal) Azoogle also noted to Spamhaus,
11 referring to spamming, "that such low lying fruit is available for huge profits". (AZ-SP 045, Exhibit C
12 to RG, under seal) It is no wonder how an email marketing company went from inception to \$50 million
13 a year, in three years. Azoogle was terminated from several ISP's for spamming, including Savvis,
14 (Bate 0853, Exhibit B to RG) and Burstnet, which resulted in Azoogle being listed on Spamhaus's
15 ROKSO, (Register of Known Spamming Operations). AZ-SP 002, Exhibit C to RG under seal.

16 ASIS Internet has received an ever increasing amount of SPAM for the past several years. The
17 cost of processing email and filtering out SPAM has grown dramatically. ASIS has had to add software,
18 hardware, staff, and network bandwidth to fight the SPAM. ASIS also currently uses a service,
19 POSTINI, to preprocess all of the mail sent to its email server, at considerable cost. (See ¶2 of the
20 Declaration of Nella White in Support of Plaintiff's Opposition to Motion to Dismiss, Docket 50,
21 courtesy copy (1) attached hereto (hereafter "Docket 50")).

22 During the months of October and November of 2005, plaintiff received in excess of 10,000
23 mortgage solicitation emails to its servers that met the definition of SPAM under the *CAN SPAM Act of*
24 *2003*. These emails were sent using obviously stolen email identities. Plaintiff continued to receive
25 emails even after the initial complaint for this action was filed, in December 2005, until January 30,
26 2006. These emails were sent with false header information, so as to make tracing the source
27 impossible. These emails were sent with subject lines that contained consistently misspelled words.
28 (See ¶3 of Docket 50). A sample of the various emails is included as Exhibit A to Docket 50 that

1 demonstrate the email identity problem and the subject line problem. A sample of one of the emails, the
2 eventual recipient would see, and the Internet site the emails directed the recipient to are also included.
3 (See Exhibits B and C to Docket 50). The ASIS recipient email I.D. is redacted to protect the privileged
4 corporate information of ASIS and to protect ASIS and the intended recipients from retaliatory
5 electronic attacks.

6 All of these emails asked the recipient to go to various specific Internet sites, such as
7 wwmort.com, bbmort.com, xxmort.com, etc., and contained a link to get there. However, once a party
8 went to any of those sites, the graphics and site information was exactly the same. See Exhibit "B" to
9 Docket 50.

10 Late at night on Thursday, October 27, 2005, Nella filled out a form on the wumort.net site,
11 using unique information regarding a fictional person, Bruce Wolf. See Exhibit "C" to Docket 50. Nella
12 chose wumort.net because it clearly had been sent to a large percentage of her customer base, listed
13 alphabetically, leading her to suspect they had been gathered by means of a Directory Harvest Attack.
14 See ¶7 Docket 50.

15 The telephone number provided by Nella White in filing the Bruce Wolf lead was attached to a
16 recording machine. The telephone number received a number of calls from mortgage brokers on
17 October 28, 2005, the day after Nella White entered the Bruce Wolf information into the wumort.net
18 website. The voice recordings were transcribed by Teresa Singleton, a clerk at Singleton Law Group.
19 See Exhibit A to Declaration of Teresa Singleton in Support of Opposition to Motion to Dismiss, Docket
20 #51 (courtesy copy (2) attached hereto).

21 From the calls received on October 28, 2005, Plaintiff's attorney was able to identify nine
22 separate mortgage companies who were responding in less than 24 hours to the Bruce Wolf lead. The
23 Bruce Wolf information was not available from anywhere else; Nella White made it up on the night of
24 October 27, 2005. See ¶7 Docket 50. Therefore, the only way for these nine mortgage brokers to have
25 gotten the information is to have received the information from the person who owned the web-site
26 wumort.net. Azoogole sold the "Bruce Wolf" lead to Quicken Loans, Aegis Lending, and another lead
27 aggregator, eLeadZ. See Azoogole's Response to Request for Admission, No. 22, and Amended
28 Admission No. 19 (Exhibit D to RG) and McVey P198, L.9-10 (Exhibit E to RG)..-

1 The “Bruce Wolf” lead was received by Quicken Loans from Azoogle as coming from
2 “*LowRateAdvisors.com*” Exhibit F to RG, QL-0116. Indeed, Quicken Loans sent an email to the
3 fictitious Bruce Wolf stating that Quicken Loans was responding to Bruce’s loan inquiry made through
4 the “lowrateadvisors.com” web page. See Exhibit F to the Declaration of Nella White in Support of
5 Motion for Summary Adjudication (hereinafter Dec. NW). (Bruce’s email address was given in the
6 process of filling out the wumort mortgage web page) Now, Quicken’s twice referencing Bruce’s
7 inquiry as coming from the lowrateadvisors.com web page is particularly telling. Azoogle operated its
8 own web property¹, “lowrateadvisors.com,” (Exhibit G to RG) and that web page, in one incarnation,
9 was nearly identical in content to the wumort web page filled out by Nella White. Docket 50, Exhibit C.
10 The only way Quicken could have referenced the Bruce Wolf lead as coming from
11 “lowrateadvisors.com” is if *Azoogle so told Quicken*. Azoogle operated a variety of other mortgage lead
12 pages, such as ChristianMortgageUSA, Bluecollarmortgage, etc, but those were not the pages Azoogle
13 referenced as generating the lead. The inference is, that Azoogle knew the “Bruce Wolf” lead came
14 from a web page that was nearly identical to its own “lowrateadvisors.com” page, given Azoogle’s
15 identification of the lead to Quicken as coming from “lowrateadvisors.com.”

16 There is further support in the record that shows Azoogle was aware it was receiving mortgage
17 leads from the wumort web page. Azoogle received its mortgage leads electronically in real time, via
18 custom Azoogle software known as “Lead Agents.” See McVey, P34, L16-P35, L23 (Exhibit E to RG)
19 and Mossanen, P24, L20-P25, L10 (Exhibit J to RG, under seal). This was true as to the leads coming
20

21 ¹ Azoogle’ site: <http://www.lowrateadvisors.com/long/index.php?affil=1828#>, is a web page that is
22 virtually the same as the web page Nella White saw in October 2005. This web page contains the following:
23 “©AzoogleAds.com Inc., All Rights Reserved.” See Exhibit H-Carl 2 Ex. C. Domain name
24 “Lowrateadvisors.com” is owned by Azoogle. <http://www.lowrateadvisors.com/long/index.php?affil=1828#>, is
25 located at IP address 209.47.46.154, which is in the range of IP addresses owned exclusively by Azoogle per
26 Azoogle’s disclosure of June 22, 2007. See Exhibit I to RG, AZ-0125 (under seal).

27 Images of each element of the page Nella White saw on October 27, 2005, appearing in the wumort.net
28 web page, also appear on the Azoogle server at:
www.lowrateadvisors.com/long/images/ln_1.jpg;; www.lowrateadvisors.com/long/images/ln_2.gif
www.lowrateadvisors.com/long/images/ln_5.gif; www.lowrateadvisors.com/long/images/ln_6.jpg
www.lowrateadvisors.com/long/images/graph.gif; www.lowrateadvisors.com/long/images/ln_right.gif
www.lowrateadvisors.com/long/images/spacer.gif; www.lowrateadvisors.com/long/images/ln_left.gif. See Exhibit H-Carl 2
Exhibit E. The source code for the wumort.net, and the Azoogle web pages all use the exact same file names for the images.
That is the file name for the image of the house is “ln_6.jpg.” The file name for the Freddie Mac graph image is “graph.gif.”
As discussed above these are the same file names used on the Azoogle lowrateadvisors.com image server. See Exhibit H-Carl
2 Exhibits B and C and D for printouts of the source code for the wumort.net and other landing pages.

1 from Seamless Media, the company Azoogle identified as producing the “Bruce Wolf” lead for Azoogle.
2 Exhibit E to RG-McVey P201, L16 and Exhibit J to RG, under seal, Mossanen P55, L16-23). Lead
3 Agents, was an electronic connection between the third party vendors mortgage landing page, and
4 Azoogle. Azoogle’s third party vendor’s landing page had to be specially configured in advance, (an
5 HTML post, it is called), to submit the leads generated on that page, to Azoogle’s Lead Agents software.
6 See Don Mathis, P169, L9-18, (Exhibit A to RG, under seal); Rick Okin P46, L16-23 and P52, L20-24,
7 (Exhibit K to RG, under seal). When Azoogle’s Lead Agents software communicated with a third party
8 vendors mortgage page, receiving a mortgage lead, Lead Agents recorded the URL, or landing page,
9 from which the lead was generated. See Marvin Hernandez P153 and 155 (Exhibit L to RG) and Rick
10 Okin, P23, L15 to P24, L2 (Exhibit K to RG, under seal). Azoogle was quite aware that it was obtaining
11 leads from the wumort copy of Azoogle’s “lowrateadvisors.com” web page. Moreover, Azoogle
12 engaged in a standard practice of allowing its third party vendors to copy (and re-host) Azoogle’s web
13 pages, for use by the third party vendor, so as to allow the third party vendor to generate leads that
14 would be sold to Azoogle. Mossanen P111, L20, P112, P118, L23-P119, L8 (Exhibit J to RG, under
15 seal). In such a process, Azoogle would not be identified on the page copied and used by the third party
16 vendor. Mossanen P112, P119, P120 (Exhibit J, under seal). It appears as the same as what occurred
17 with the wumort page visited by Nella White.

18 Azoogle received the lead at “10/28/05 12:50 PM PST,” within an hour or so of when Nella
19 White entered the information on the wumort.net site. Exhibit I to RG, AZ-0022. This is consistent
20 with Lead Agents receiving the lead in “real time” as testified to by Ryan McVey.

21 Quicken loans received assurances from Azoogle that:

22 **“Mortgage leads are generated by our own web properties allowing greater**
23 **quality control, submitted by nationwide consumers, who are ready to buy – leaving**
24 **you with the invaluable opportunity to close!” Exhibit M to RG, QL-0023, under seal.**
(emphasis added)

25 The “lowrateadvisors” web page has a long history of having traffic driven to it by spam:

- 26 1. In the FTC v Optin Global (USDC, Northern District of California, 3:05-cv-
27 01502-SC) matter, the “lowrateadvisors” page there was listed by the FTC as one
of the pages advertised via spam. See Exhibit N to RG, P132, Item C and P216.
- 28 2. In May of 2005, Alex Zhardanovsky, founder of Azoogle.com, was accused of
mortgage refinance spamming using the same house image, (as appeared on

1 Nella's page) on a blog linking to the Azoogle.com image. Exhibit O to RG. The
2 archive of the blog can be found at <http://www.webservertalk.com/archive154-2005-5-1074010.html>.

- 3 3. Savvis was Azoogle's internet access provider, until Savvis canceled Azoogle's
4 service for spam violations. Prior to termination, Savvis forwarded to Azoogle
5 the specific spam complaints. Several of these complaints were because of a
6 spamadvertised site, "lowrateadvisors.com"... See Exhibit P to RG, Bate Stamp
7 864, 1087, 1088.
- 8 4. Azoogle corresponded with Spamhaus over a period of years, in an effort to get
9 removed from Spamhaus's ROKSO list. Within that correspondence, Spamhaus
10 notes that part of the listing is due to spam advertising of "lowrateadvisors.com."
11 See Exhibit C, AZ-SP 050, under seal).
- 12 5. In the within case, as noted above in some detail, the web site Nella White went to
13 and filled in the Bruce Wolf information was nearly identical to Azoogle's
14 Lowrateadvisors.com site. When Don Mathis, Azoogle's Chief Operating
15 Officer, was shown, during his deposition, that the image of the house on
16 Azoogle's proprietary site, and the site Nella White went to, *were identical*, Mr.
17 Mathis' response was, "*son of a bitch*." Mathis, P268, L13 (Exhibit A to RG).
- 18 6. One of Azoogle's marketing affiliates, Scott Tesler, copied the
19 lowrateadvisors.com site from Azoogle's server, and hosted it on his own server,
20 at "lowrateadvisors.net." Scott then used it to generate mortgage leads. Joe
21 Speiser, stated, under oath, the "lowrateadvisors.net" site was not theirs, was
22 being used without authorization, and that a cease and desist letter was sent out.
23 (Speiser, P68 L10-14, Exhibit B to RG) Now Scott states Azoogle had his contact
24 information, and never said a word to him about his unauthorized use of
25 Azoogle's lowrateadvisors.com page. Please see Declaration of Scott Tesler,
26 Exhibit Q to RG). Azoogle clearly does nothing to prevent, even by its affiliates,
27 the unauthorized use of Azoogle's landing pages.

18 Azoogle states it received the Bruce Wolf lead from its third party vendor Seamless Media.
19 Exhibit R to RG, Azoogle's response to Interrogatories at 15:21-24. Azoogle has provided a third party
20 "advertising insertion order" with terms and conditions that covers its agreement with Seamless Media.
21 Exhibit I to RG, AZ-018-021, under seal. Note that the agreement allows for the use of email
22 advertising to generate the leads. AZ-018 (Exhibit I to RG, under seal). Julian Mossanen testified that
23 portion of the "Insertion Order" indicates what forms of advertising the third party vendor is permitted
24 to use to generate the leads. Mossanen P42, L13 to P44, L14 (Exhibit J to RG, under seal) Indeed,
25 Azoogle *pre-paid* Seamless Media for 50% of the leads that Seamless was going to generate for
26 Azoogle, using email marketing. (AZ-05, Exhibit I to RG, under seal)

27 There is ample evidence the emails at issue in this case came from the same source. Of the
28 12,756 emails produced by Plaintiff, 1578 of those emails contain a link to wumort.net or wumort.com.

1 See Declaration of Carl Scoles RE Supplemental Disclosure Six Amended (hereafter Carl-#6) and
2 attached Exhibit "A," Sheet 4, "E-mail counts-per domain" attached as Exhibit S to RG. Of the emails
3 that contained a link to something other than wumort.net or wumort.com, such links within the emails
4 resolved to pages that were hosted on the exact same IP address as the wumort.com and wumort.net or
5 hosted images that were the same as those on wumort.net. See Carl#6-Exhibit "A," Sheet 3, "IP's &
6 related domains" (Exhibit S to RG).

7 Moreover, the wumort.net and wumort.com emails are exactly the same in appearance, even to
8 the point of the same misspellings, except for the different senders, recipients and URL link. These
9 emails share *many* similarities to the emails that do not resolve to wumort.com or wumort.net. These
10 two factors together, sharing of IP address of the internal link within the emails, and the similarity of the
11 emails to one another, indicates the 12,756 emails, (at a minimum 1578 emails) came from the same
12 source and directed the recipient to the same group of web sites. See Declaration of Josh Mohland in
13 response to Court Ordered Interrogatories (hereinafter JM1) attached as Exhibit T to RG.

14 **2. Plaintiff is an Internet Access Provider (hereafter IAP) and Email Service**
15 **Provider (hereafter ESP).**

16 Nella White, President and CEO of ASIS, in her Declaration in Support of Plaintiff's Motion for
17 Summary Adjudication of Issues (hereafter Dec of NW) Para. 2 and 3 state that ASIS Internet Services,
18 Inc. (hereafter ASIS), is a corporation in the business of providing access to the Internet and email to
19 consumers and businesses in Northern California. ASIS was started in 1995 and had just under 1,000
20 Internet access and email customers in 2005. Nella White states in her deposition Pg. 76, L. 10 (See
21 Exhibit U to RG) that ASIS is an Internet Service Provider.

22 ASIS owns various domain names used to provide internet and email services. See Dec. of NW
23 Para. 4 and Exhibit A for printouts of WHOIS reports indicating ownership of six domain names used in
24 the provision of access to the Internet and email services.

25 Plaintiff, in response to Defendant Quicken's Request for Production No. 2, provided to all
26 parties the following documents: Articles of Incorporation of ASIS INTERNET SERVICES; ASIS's
27 Business License; various vendor invoices related to providing Internet and email services; and sample
28 Customer Invoices (customer names redacted) for both Internet and email services. See Para. 6 and

1 Exhibit B to Dec. of NW.

2 ASIS has provided bandwidth graphs and Server Configuration files attached as Exhibit F to
3 Plaintiff's Expert Disclosure of Jeffrey Posluns. See Para. 7 and Exhibit C, under seal, to Dec. of NW.

4 These documents and declarations provide undeniable proof that ASIS is and was, at the time of
5 the incidents in this case, a provider of access to the Internet and email services.

6 **3. The emails at issue were sent to ASIS email accounts and that they were**
7 **received by ASIS.**

8 During the months of October of 2005 through January of 2006, Plaintiff received in excess of
9 10,000 emails to its servers that met the definition of SPAM under the *CAN SPAM Act of 2003* and the
10 *California Business and Professions Code* §17529.5. (Plaintiff has recently re-counted the emails
11 using a program specifically designed to count the multiple "To" and "CC" addresses contained in the
12 emails.) The emails are attached in electronic form, under seal, with instructions for viewing as Exhibit
13 E to Dec. of NW. (In addition, Exhibit E contains a second disc that can be loaded in any XP computer
14 and read without loading them into a browser on the user's computer.) The emails are provided under
15 seal as they contain the un-redacted email accounts of ASIS customers. These emails were initially
16 provided to Defendants in Plaintiff's Supplemental Disclosure on January 11, 2007. (See Exhibit E to
17 Dec. of NW). The count reached when recounting the emails is 12,756. See Declaration of Josh
18 Mohland in Support of Court Ordered Interrogatories [hereafter JM1], ¶5 Exhibit T to RG).

19 Nella White described the receipt of the emails in her original declaration, Docket 50, Para. 2 –
20 5, and email samples provided in Exhibit A.

21 All of the emails at issue in this case were sent to email accounts at "asis.com." This can be
22 confirmed by reviewing the emails. Nella in her prior declaration (Docket 50) and in her current
23 declaration declares that ASIS received these emails. See Dec. of NW, Para. 5.

24 Therefore, there is no dispute the emails were sent to Plaintiff's email accounts and received by
25 Plaintiff's email service.

26 **4. The subject emails contain false header information.**

27 The email headers at issue in this case contain false header information. The originating or
28 source IP addresses (in the email's header information) do not correspond with the sending email

1 domain names, (the “sent from” field in the email). In most cases the sending email domains are not
2 even in the same country as the originating IP addresses. See Dec. of Josh Mohland (hereinafter JM2),
3 ¶2 and Exhibit A (Exhibit V to RG) for a comparison of the sending domain name locations and IP
4 locations. Also see Expert Disclosure of JP, P6-7, ¶C, Exhibit W to RG.

5 The *CAN SPAM Act* provides that an email is in violation if it contains header information that
6 is materially false or misleading. The simple method for determining whether these emails were sent
7 using stolen email accounts would have been to contact the senders and verify whether they sent them.
8 In this case with over 1,400 senders that was both impractical and impossible. Impossible because most
9 of the emails were sent from domain names such as yahoo.com, hotmail.com, gmail.com, etc. These
10 accounts can be set up in minutes with no verifiable information regarding the applicant. Most of these
11 email accounts are set up with no real information, making investigation impossible. The mere fact that
12 the sender is untraceable probably represents a violation of the *CAN SPAM Act*. However, Plaintiff
13 undertook a more sophisticated method of proving the emails contain false headers.

14 First, it is an accepted industry standard, that the sending domain name must match the sending
15 IP address. In 2003, Microsoft created the Sender ID Framework (hereafter SIDF) email verification
16 process. Microsoft implemented SIDF service wide in Hotmail in January 2005. Other services such as
17 GoDaddy have also implemented SIDF. SIDF uses the presumption that the sending IP address will
18 match the sending domain name in order to establish a high level of confidence that the email is from
19 the sender identified in the send field. See JM2 (Exhibit V to RG), Para. 4 and Exhibit B for a copy of
20 the Sender ID Framework White Paper from Microsoft. The SIDF is consistent with and complies with
21 the Industry Standard Simple Mail Transport Protocol (SMTP) RFC 2821. See JM2, Exhibit B, ¶2.1 the
22 SMTP Model Basic Structure (Exhibit V to RG).

23 For most services such as Hotmail, Yahoo, Gmail, and AOL it is impossible for a user sending a
24 valid email through these services without the email including a valid IP address from the service, since
25 it must pass through or be sourced from the services mail server. For other services it is not impossible
26 but it is highly unlikely that an email will contain an originating IP address foreign to the email service.
27 For every service it is inconceivable that the email service would route an email from someone in
28 California to someone in California through China, Germany or South Korea. As is demonstrated in

1 Exhibit A to JM2, (Exhibit V to RG) See also WHOIS report for Yahoo.com and other services as
2 Exhibit C to JM2 (Exhibit V to RG). Only 2 of the subject emails contain IP addresses that match the
3 sending domain name. Most are not even from the right country.

4 All of the IP ranges owned by Yahoo! Inc. can be determined by a search of the ARIN database.
5 See Exhibit D JM2 (Exhibit V to RG). None of the emails at issue show an originating address within
6 an IP range owned by Yahoo! Inc. 2134 of the emails at issue contain sending domain names of
7 “yahoo.com” but do not contain an originating IP address owned by Yahoo! Inc. A check of the other
8 services such as Gmail, Hotmail, etc., supposedly originating the emails, indicates that the emails did not
9 originate from IP addresses owned by those services. See ¶2(B) and Exhibit A, P4 – 23, to JM1 (Exhibit
10 T to RG).

11 A second industry standard available for determining whether an email is valid is the
12 DomainKey authentication system. Yahoo created and implemented a standard for authenticating
13 emails for their service called DomainKey authentication prior to 2004. See Exhibits E and F to JM2
14 (Exhibit V to RG), RFC 4870 and 4871 describing the DomainKey process. This standard requires that
15 a Domainkey authentication code be included in the header of every email from Yahoo. This standard
16 was adopted by many of the large email services including Gmail (Google), and AOL in 2004. An
17 email from Yahoo, Gmail or AOL must contain a DomainKey to be valid and the DomainKey can be
18 verified by checking with the sending entity’s server (i.e. Yahoo, Gmail, and AOL). Only 120 of the
19 emails contain a DomainKey of any kind. Several contain DomainKeys that are improperly formed. A
20 check of the DomainKeys indicates that none of these Domainkeys are valid. ¶25 of JM2 (Exhibit V to
21 RG).

22 Finally, all of the emails at issue were sent in a non-random fashion from different personal
23 computers in alphabetical order of the intended recipients. That is the emails were sent in bursts from
24 different senders in alphabetical order of ASIS’s customer email account list. See JM1, ¶F and P25–26
25 of Exhibit A (Exhibit T to RG). The characteristics of the emails are almost identical, within three
26 categories. (While this information is discussed in detail in JM1 and Expert Disclosure of JP, it can also
27 be easily verified by looking through the emails provided in Exhibit E to Dec. NW.) This indicates that
28 the emails were being sent in a coordinated fashion through some 1,026 separate IP addresses. The only

1 way this can be accomplished is through a botnet controlled by a single sender. See JM1, ¶F and P25–
2 26 of Exhibit A (Exhibit T to RG). Also see Expert Disclosure of JP, P12-13, ¶G (Exhibit W to RG).
3 Since it is very likely that a botnet was used to send the emails, this provides further proof the sending
4 email accounts as well as the sending computers were hijacked to send the emails.

5 **5. The Subject emails contain false or misleading subject lines.**

6 The criteria for judgment of whether an email contains a misleading subject line is that it contain
7 some form of false or misleading statement or that it purposefully attempts to trick the recipient into
8 viewing the email.

9 All of the emails contain an offer to refinance the recipients mortgage, this is the only offer
10 contained in the emails. (See Exhibit E to NW, the emails at issue in this case.)

11 9,163 of the emails contain subject lines that claim the recipient has either been approved
12 or pre-approved for a mortgage. These emails contain a link that offers to get
13 brokers to call the recipient, after providing confidential information. These subject
14 lines are therefore misleading or completely false and intended to get the recipient
15 to open the emails.

16 42 of the emails contain subject lines that claim that there is a pre-existing application on
17 file. Since the emails are trying to get a recipient to fill out a form to get refinance
18 quotes, this cannot be a truthful statement.

19 36 of the emails contain subject lines that describe places of interest, such as “Vacation
20 homes w/oceanview for L;e:ss.” Since this has nothing to do with the offer in the
21 email it is a misleading subject line intended to get the recipient to open the email.

22 352 of the emails contain subject lines that have nothing to do with mortgages or
23 refinance, such as “Message subject” or “Re: Office Admin.”

24 19 of the emails contain subject lines that refer to making money, such as “Make \$...”

25 23 of the emails contain subject lines that appear to be asserting a prior relationship, such
26 as “More Information needed” or “Urgent matter.”

27 78 of the emails contain subject lines that claim that there is important information, such
28 as “Important Email. Details inside.” This subject line is clearly intended to trick
the recipient into opening the email.

24 of the emails contain no subject line at all.

25 See Exhibit H (Car12), ¶3 and Exhibit A, for a complete breakdown on the subject lines of the
26 emails. There is no dispute that 9,737 of the emails have false or misleading subject lines. Therefore,
27 Plaintiff is entitled to summary adjudication of this issue.

28 ///

1 **6. The subject emails do not contain a valid unsubscribe option and a physical**
2 **opt-out address.**

3 None of the emails contain a physical address where the recipient can contact the sender to
4 discontinue receiving these emails. This is in direct violation of 15 *USC* 7704(a)(5)(A)(iii). See the
5 subject emails in Exhibit E to NW and Exhibit H to RG, Carl2, ¶3.

6 Within the 12,756 emails, only 131 of the emails have what may be considered to be a valid
7 unsubscribe section. 1,847 of the emails have what could be considered questionable unsubscribe links.
8 10,662 of the emails have what are considered invalid unsubscribe references and links. The rest of the
9 116 emails literally have no unsubscribe link, meaning that there is no actual hyperlink in which to
10 unsubscribe. See ¶4 and Exhibit A to Carl2-Exhibit H to RG. Also see Exhibit E to NW.

11 12,625 of the emails do not contain a valid unsubscribe link. All 12,756 of the emails do not
12 contain a physical opt-out postal address. Therefore, Plaintiff is entitled to summary adjudication of this
13 issue.

14 **7. The emails at issue were not solicited by the intended recipients.**

15 Plaintiff has provided evidence that the emails were not solicited. First, Plaintiff provided
16 Defendant with a list of some 246 inactive email accounts owned by Plaintiff that received a significant
17 portion of the emails at issue in this case. See Exhibit X to RG, Plaintiff's Response to Defendant's
18 Request for Production No. 4 and the emails list attached to the Response (Exhibit Y to RG, under seal).
19 Some of the emails were sent to internal service email accounts at **ASIS**. Since these email accounts
20 were not active, and some had never been used as external email accounts, they could not have solicited
21 mortgage refinance advertisements from Defendant. Second, Defendant has stipulated, under court
22 order, that they do not have any opt-in data that relates to the emails in this case. (Docket 249, Courtesy
23 copy (3) attached). Moreover, Defendant has produced no evidence whatsoever that any ASIS client
24 solicited to receive the subject emails. Solicitation is Defendant's affirmative defense and Defendant
25 has provided no facts to support this defense. Therefore, Plaintiff is entitled to summary adjudication of
26 this issue.

27 **B. ARGUMENT**

28 **1. Summary Adjudication of issues and defenses is within the authority of the Court.**

 The court has authority to rule on both defenses and issues in this action.

1 The court has authority based on *FRCP* Rule 56(a)(c) and (d) to rule in summary judgment on
2 Plaintiff's claims. This includes defenses claimed by Defendants as well as issues inherent in Plaintiff's
3 claim. *FRCP* Rule 56(d) states that if summary judgment is not "rendered on the entire action", the
4 court should determine what facts are not genuinely at issue. These facts are then considered established
5 in the action. *Wang Laboratories, Inc. v. Mitsubishi Electronics, America, Inc.*, 860 F.Supp. 1448,
6 1450 (CD CA 1993); also see *Williams v. Sinclair*, 529 F2d 1383 at (9th Cir. 1975) for the proposition
7 that after denying summary judgment a court may be asked for an order that deems certain facts
8 established.

9 In cases that involve complicated fact patterns and multiple causes of action,
10 summary judgment may be granted as to some causes of action but not as to
11 others or as to some issues but not as to others, and as to some parties but not as to
12 others ... a careful and meticulous analysis first by the parties, but ultimately by
the district court will aid significantly in preventing the waste of private and
judicial resources and time.

13 *Barker v. Norman*, 651 F.2d 1107 at 1123 (5th Cir., 1981).

14 Therefore, in complicated cases, such as this matter, where the case is not fully adjudicated on
15 the facts, the Court should determine what facts are established to reduce time at trial and prevent the
16 waste of judicial resources.

17 **2. Standard for Summary Judgment.**

18 Upon a showing that there is no genuine issue of material fact the court may grant summary
19 judgment on all or any part of Plaintiff's claim. *FRCP* Rule 56(a). *FRCP* Rule 56(c) states that the court
20 shall grant summary judgment if:

21 the pleadings, the discovery and disclosure materials on file, and any affidavits
22 show that there is no genuine issue as to any material fact and that the movant is
entitled to judgment as a matter of law.

23 Material facts are determined by the substantive governing law. The moving party has the
24 burden of demonstrating the absence of a genuine issue of fact for trial. *Anderson v. Liberty Lobby,*
25 *Inc.*, 477 U.S. 242 at 248 and 249 (1986).

26 **3. There is no factual or legal basis for the defense asserted by Defendant that
Plaintiff assumed the risk.**

27 Defendant has asserted that Plaintiff assumed the risk and contributed to its own damages.

28 First, Plaintiff did not make a claim for actual damages in its Complaint. Plaintiff prayed for

1 statutory and liquidated damages, not actual damages. See Prayer, Pg. 14 Second Amended Complaint,
2 Docket 117 (hereafter SAC). Statutory and liquidated damages in this case are a penalty enacted by the
3 federal and California state legislatures to punish parties for spamming and false advertising. 15 USC
4 7701 et seq. and *California Business and Professions Code* §17529.5. The general intent of the law is
5 to reduce the amount of SPAM sent by providing various parties including IAPs the right to enforce
6 penalties.

7 Second, Defendant has provided no viable legal basis to conclude Plaintiff's alleged assumption
8 of the risk is in anyway applicable to the present action. Plaintiff is in the business of operating an
9 Internet and email service. Assumption of risk and contribution are affirmative defenses *to negligence*
10 *claims*. It is clear these defenses do not apply to statutory violations. In similar situations the Court has
11 found that assumption of risk and contribution do not apply to statutory violations. *Crane v. Cedar*
12 *Rapids & I. C. Ry. Co.*, 395 U.S. 164 at 166 (1969), finding that an employee suing under the Federal
13 Employer's Liability Act is relieved of proving proximate cause and the employer is deprived of the
14 defenses of contributory negligence and assumption of risk. The employee was only required to prove
15 his injury was a result of the employer's violation of the act. The Court held in *Crane* that the recovery
16 of damages for a breach of duty came from common law, and therefore the Court has consistently held
17 that the defenses of assumption of risk and contributory negligence are left to state law. *Id.* at 167.

18 The California Supreme Court has held:

19 assumption of risk is in reality a form of contributory negligence 'where a
20 plaintiff unreasonably undertakes to encounter a specific known risk imposed by a
21 defendant's negligence

22 *Knight v. Jewett*, 3 Cal.4th 296, 308 (Cal. 1992).

23 Even assuming Plaintiff's claims sounded in negligence, the doctrine would not apply. In cases
24 of negligence a plaintiff must know the consequences of the defendant's negligence and reasonably or
25 unreasonably assume the consequences. Further, in order to bar recovery, a defendant must show that
26 the plaintiff acted in a manner unreasonable under the circumstances. *Alber v. Owens*, 66 Cal.2d 790 at
27 799 (Cal. 1967). Defendant has offered no evidence that anything Plaintiff did was unreasonable.

28 Plaintiff has not and cannot assume the risk, in operating its business, that unknown parties will
violate the law by sending SPAM to its servers. Defendant's argument attempts to shift the burden of

1 prevention of the violation, sending spam, on to the plaintiff. The *CAN SPAM Act* and The California
2 Statute provide for penalties calculated for each spam email sent. 15 *USC* 7704 and 15 *USC* 7706, and
3 *California Business and Professions Code* §17529.5. The *CAN SPAM Act* provides methods for
4 mitigating these penalties by actions taken by the spammer, such as procuring opt-in consent. 15 *USC*
5 7706(g)(3)(D). It is inconceivable that the legislatures intended to turn the statutes on their heads by
6 requiring that a plaintiff demonstrate that he did not assume some risk in order to inflict the penalties on
7 a defendant caught spamming. Judge Conti wrote:

8 “The court further finds that the affirmative defense which Defendants propose to
9 add to their answer runs contrary to the structure of the CAN SPAM Act as a
10 whole, shifting from the spammer to the receipt of SPAM the responsibility to
11 limit receipt of unwanted spam.”

12 “By requiring recipients, rather than spammers, to take actions necessary to limit
13 their receipt of spam, Defendants’ proposed affirmative defense would turn this
14 section of the Act on its head.” *Phillips v. Netblue, Inc.*, Slip Copy, 2006 WL
15 3647116 at 4 (N.D.Cal.,2006) (Courtesy copy (4) attached).

16 Therefore, since there is no legal basis for Defendant’s affirmative defense, the court should
17 strike Defendant’s affirmative defense of assumption of risk and contribution.

18 **4. There is no factual or legal basis for the defense asserted by Defendant that**
19 **any loss incurred by Plaintiff was proximately caused by the acts of third**
20 **parties or non-parties.**

21 Defendant has asserted that Defendant is not liable because the injuries suffered by Plaintiff were
22 caused by a third party that Defendant did not control. Defendant has misinterpreted the *CAN SPAM*
23 *Act* and *California Business and Professions Code* as to how liabilities are incurred by Defendant. The
24 *CAN SPAM Act* does not require a showing of agency, rather, its terms create vicarious liability within
25 its own special provisions.

26 The *CAN SPAM Act* states that it is unlawful for “any person to initiate the transmission,” of
27 emails in violation of the Act. 15 *USC* 7704(a)(1). The term “initiate” means: “to originate or transmit
28 such message or to procure the origination or transmission of such message...” 15 *USC* 7702(9). The
term “procure” means: “intentionally to pay or provide other consideration to, or induce, another person
to initiate such a message on one's behalf.” 15 *USC* 7702(12). (emphasis added)

Therefore anyone who induces another to send commercial electronic mail messages is
potentially liable for the penalties assessed by the Act. There is no requirement that defendant control

1 the third party in order for liability to be incurred, only that the third party was induced by the defendant.

2 This argument is further supported by the special definition of *procure* allowed to plaintiff
3 IAPs: “*with actual knowledge, or by consciously avoiding knowing, whether such person is*
4 *engaging, or will engage, in a pattern or practice that violates this chapter.*” 15 USC 7706(g)(2).

5 This language indicates that the defendant does not even have to know that the party they have
6 induced is violating the Act, only that the defendant has consciously avoided knowing the fact. This
7 implies a very low burden of proof on the part of plaintiff, that does not include proving knowledge or
8 intent on the part of the defendant doing the inducing. A plaintiff need only show a laxity in the
9 procurement management of the relationship. Defendant’s argument that it is not liable due to acts of
10 third parties it did not control, is irrelevant as a matter of law.

11 Defendant has provided the email insertion order with Seamless Media that Defendant claims is
12 responsible for acquiring the “Bruce Wolf” Lead. This advertising insertion order allows for the use of
13 emails, for which Defendant agrees to pay Seamless Media a bounty for each lead acquired. And
14 indeed, for which Azoogole pre-paid for the email generated leads, *in advance*. Therefore Defendant has
15 provided evidence that it induced Seamless Media to send emails.

16 Defendant has admitted it did nothing whatsoever to police its third party vendors to prevent
17 spamming, other than to get them to sign an agreement. Julian Mossanen hired and managed Azoogole’s
18 third party vendors, such as Seamless Media. Mr. Mossanen testified in his deposition when queried if
19 Azoogole policed the third party vendors, they did nothing. See Exhibit J to RG, Mossanen Depo., P129,
20 L2-19 (under seal)

21 Defendant has further admitted that it cannot produce any signed agreements with any of its third
22 party vendors other than the Seamless Media Agreement. Exhibit Z to RG, Declaration of Azoogoleads
23 General Counsel, David Graf (Docket 258). Defendant has provided a list of 63 third party vendors.
24 Exhibit I to RG, AZ 0131–132 (under seal). The point being, Azoogole, not being able to produce
25 enforceable contracts with its vendors, could not enforce those contracts if it wanted to. If Azoogole had
26 intended to be able to enforce the contracts with its third party vendors, it would have properly archived
27 them. Azoogole had no intention of ever enforcing its third party vendor contracts.

28 Therefore, Defendant has provided evidence that they induced the emails and that they

1 consciously avoided knowing what their third party vendors were doing.

2 As discussed above proximate causation does not apply to statutory violations. Plaintiff need
3 only show that Defendant through his actions violated the statues and that Plaintiff suffered adverse
4 affect as a result of that violation. This is exactly what was intended by the legislature in enacting the
5 *CAN SPAM Act* of 2003 to prevent unwanted SPAM by imposing harsh penalties.

6 “The purposes of this legislation are to: ... (iv) prohibit businesses from
7 knowingly promoting, or permitting the promotion of, their trade or business through e-
8 mail transmitted with false or misleading sender or routing information.” **SENATE
REPORT NO. 108-102**, 2004 U.S.C.C.A.N. 2348, July 16, 2003, Courtesy copy (5)
attached.

9 *California Business and Professions Code* §17529.5 has a completely different requirement for
10 assessing liability. The *California Business and Professions Code* places liability on the advertiser: “It
11 is unlawful for any person or entity to advertise...” *California Business and Professions Code*
12 §17529.5(a). Therefore, Plaintiff must show that Defendant advertised in the email, not that Defendant
13 controlled the email sender.

14 The concept of control is relevant to a discussion of an agency or employer relationship. No
15 agency or employer relationship is required to show liability in a SPAM suit. Therefore the issue of
16 control is irrelevant. Defendant’s affirmative defense should be struck as a matter of law.

17 **5. There is no factual or legal basis for the defense asserted by Defendant that**
18 **Plaintiff’s claims are barred by the doctrine of unclean hands.**

19 The doctrine of unclean hands does not apply since Plaintiff has shown no bad intent prior to or
20 in the course of bringing this lawsuit.

21 The doctrine of unclean hands bars relief to a plaintiff who has violated conscience, good faith or
22 other equitable principles in his prior conduct, as well as to a plaintiff who has dirtied his hands in
23 acquiring the right presently asserted. Bad intent is the essence of the defense. *Dollar Systems, Inc., v*
24 *Avcar Leasing Systems, Inc.*, 890 F.2nd 165, 173 (9th Cir. 1989).

25 Plaintiff has detected the emails sent, preserved those emails for evidence and proceeded to
26 discover all of the parties involved. Plaintiff has included all of the parties identified who were
27 materially involved in the spamming operation as defendants in this suit, or reached settlement
28 agreements with those parties. Plaintiff, an IAP and Email Service Provider, has a legislative grant of

1 standing to bring this suits to recover penalties against those causing the adverse affect. 15 *USC*
2 7706(g)(1) and *California Business and Professions Code* §17529.5(b)(1)(A)(ii). As discussed above
3 these statutes are intended to punish defendants in order to prevent spamming.

4 Even if it were shown that **ASIS** modified its spam filtering service for the sole purpose of being
5 able to file suit against those entities sending spam to **ASIS**, such conduct cannot be said to violate
6 conscience, good faith, or any other equitable principle. No bad intent can be inferred or implied to
7 Plaintiff by enforcing the prevention of SPAM as defined in the applicable statutes.

8 Again, Azoogle’s affirmative defense seeks to place the burden of avoiding receipt of unlawful
9 spam on the recipient. Per Judge Conti’s instruction discussed above, this requirement would “turn the
10 Act on its head.” *Phillips v. Netblue, Inc.*, Slip Copy, 2006 WL 3647116 at 4 (N.D.Cal.,2006)

11 Defendant’s affirmative defense of unclean hands is irrelevant as a matter of law.

12 **6. There is no factual or legal basis for the defense asserted by Defendant that**
13 **Plaintiff has failed to mitigate damages, if any.**

14 Defendant’s affirmative defense raises two issues: whether the doctrine of mitigation of damages
15 applies to an award of statutory damages under the *CAN SPAM Act*; and whether the doctrine of
16 mitigation of damages applies to an award of damages under the *California Business and Professions*
17 *Code* §17529.5. The Northern District Federal Court has held in a similar matter that in neither case
18 does the doctrine apply. *Phillips v. Netblue, Inc.*, Slip Copy, 2006 WL 3647116 at 2-6 (N.D.Cal.,2006),

19 The doctrine of mitigation of damages requires that an injured Plaintiff employ reasonable
20 diligence to avoid aggravating the injury or increasing the damage.

21 In *Phillips* the court reasoned that the statutory damages allowed in the *CAN SPAM Act* are a
22 penalty intended to curb spam activity. *Phillips v. Netblue, Inc.*, Slip Copy, 2006 WL 3647116 at 3
23 (N.D.Cal.,2006); citing 15 *USC* 7704, 15 *USC* 7706, 15 *USC* 7703, and **S. Rep. 108-102**, 108th Cong.
24 (2003). A statutory penalty can be either a method to compensate the victim or to penalize the
25 defendant. In the case of the *CAN SPAM Act* the language clearly indicates an intent to penalize the
26 defendant.

27 The court in *Phillips* further reasoned that since the statutory penalty has “overwhelmingly focus
28 on the relative wrongfulness of the defendant's behavior,” that the doctrine of mitigation of damages

1 cannot possibly apply to statutory damages under the *CAN SPAM Act*. *Phillips v. Netblue, Inc.*, Slip
2 Copy, 2006 WL 3647116 at 4 (N.D.Cal.,2006); citing *Nintendo v. Dragon Pacific International*, 40
3 F.3d 1007, 1011 (9th Cir.1994); and *Moothart v. Bell*, 21 F.3d 1499, 1506-07 (10th Cir.1994).

4 Since the *CAN SPAM Act* focuses on the wrongfulness of the defendant's actions and not the
5 reasonableness of actions taken by the plaintiff, the doctrine of mitigation of damages cannot apply.

6 The *Phillips* court also found that the liquidated damages allowed in *California Business and*
7 *Professions Code* §17529.5 are statutory penalties and different from the actual damages allowed in the
8 statute. *Phillips v. Netblue, Inc.*, Slip Copy, 2006 WL 3647116 at 4 (N.D.Cal.,2006); citing *Beeman v.*
9 *Burling*, 216 Cal.App.3d 1586 at 1589 (Cal.App. 1 Dist.,1990); and *Turnbull & Turnbull v. ARA*
10 *Transportation, Inc.*, 219 Cal.App.3d 811 at 826, 268 Cal.Rptr. 856 (Cal.App.3.Dist.,1990). In finding
11 that the damages were in fact penalties the court determined that the doctrine of mitigation of damages
12 did not apply to liquidated damages under *California Business and Professions Code* §17529.5.
13 *Phillips v. Netblue, Inc.*, Slip Copy, 2006 WL 3647116 at FN5 (N.D.Cal.,2006).

14 Therefore, Defendant's affirmative defense of mitigation of damages is not applicable and
15 should be barred as a matter of law.

16 **7. There is no factual or legal basis for the defense asserted by Defendant that**
17 **damages, if any, were proximately caused by Plaintiff.**

18 The defense of proximate cause attempts to shift the burden to Plaintiff for its injuries by
19 showing Plaintiff did something that actually caused its injures. Since Plaintiff has done nothing but run
20 its business in a legal manner and complain of illegal activities by defendants this defense cannot apply.

21 Proximate cause is generally defined in common law as an act from which an injury results as a
22 natural, direct, uninterrupted consequence and without which the injury would not have occurred.
23 Proximate cause limits a defendant's liability for his negligence to the foreseeable consequences
24 reasonably related to the negligence. Originally defined in the famous case of *Palsgraf v. Long Island*
25 *Railroad Co.*, 248 N.Y. 339, 162 N.E. 99 (1928). To claim that plaintiff was the proximate cause of its
26 injuries attempts to turn the definition around and place responsibility on Plaintiff. Normally this would
27 amount to a claim of contributory or comparative negligence on the part of Plaintiff. No such claim or
28 defense has been made by Defendant. This is not a case of negligence, Plaintiff has alleged violations of

1 statute. Therefore it is unclear how a defense of proximate cause applies at all.

2 As noted above, Judge Conti has made clear that defenses to negligence claims, such as
3 mitigation of damages, do not apply to statutory claims such as CAN-SPAM.

4 **8. There is no factual or legal basis for the defense asserted by Defendant that**
5 **Plaintiff invited and consented to the acts of Defendant. There is no factual**
6 **dispute that the emails were not solicited by the intended recipients.**

7 See discussion above for mitigation of damages and proximate cause. Defendant has provided
8 no legal or factual basis to support a contention that Plaintiff some how invited or consented to
9 Defendant's action. Affirmative Consent or Solicitation is a partial defense to the *CAN SPAM Act* and
10 not an element of the cause of action. Therefore, Defendant has the burden of proving solicitation.

11 There is clear evidence that Defendant does not have any evidence that any emails were solicited
12 by Plaintiff or its customers. Plaintiff has provided a list of email accounts, that received the emails, that
13 were closed at the time of the action or have never been used, and hence could not have opted in to
14 receive the subject spam. See Exhibit X to RG, Plaintiff's Response to Defendant's Request for
15 Production No. 4 and the email list (Exhibit Y under seal).

16 Defendant has stipulated that *they do not have any proof of opt-in by the intended recipients of*
17 *the emails.* (Docket 249).

18 Even if Defendant could prove that the emails were solicited that evidence does not represent a
19 defense to a violation of 7704(a)(1). Primarily because if the email header information is false it does not
20 identify the party to whom the affirmative consent was granted. In addition, 15 *USC* 7704(a)(1) allows
21 for a violation for sending commercial, transactional or relationship emails. A transactional email is
22 defined as a relationship where the party has requested email or established a business relationship. 15
23 *USC* 7702(17). 15 *USC* 7704(a) does not even mention affirmative consent as a defense, except when
24 subsequently provided after a violation of 15 *USC* 7704(a)(4). It is therefore very likely that the
25 legislature did not mean affirmative consent as a defense to 15 *USC* 7704(a)(1).

26 Therefore, there is no evidence to support a defense that Plaintiff invited or consented to the acts
27 of Defendant. This defense should be barred as a matter of law.

28 ///

///

1 **9. There is no factual or legal basis for the defense asserted by Defendant that**
2 **Plaintiff waived any claim or cause of action against Defendant.**

3 Defendant has not specified what or how Plaintiff has waived its claims.

4 Waiver may occur when a party fails to assert its claim within a prescribed period. However,
5 Plaintiff filed its complaint against Defendants in less than a month after the incident started. See
6 Complaint. Plaintiff added Defendant Azoogle as a Defendant when they were discovered and within
7 six months of the Original complaint in the First Amended Complaint. See First Amended Complaint
8 (hereafter FAC). The *CAN SPAM Act* does not specify a statute of limitations for actions brought.
9 Therefore, since the *CAN SPAM Act* was enacted after 1990 the federal catch all time limitation of four
10 years applies. 28 *USC* 1658(a); *Jones v. R.R. Donnelley & Sons Co.*, 541 U.S. 369, 369 (2004). No
11 decision concerning the statute of limitations has been offered by the California Courts. However,
12 *California Business and Professions Code* §17529.5 is an action for a penalty for violation of a statute
13 therefore *California Code of Civil Procedure* §340(a) may apply and the action must commence within
14 one year. Otherwise, *California Code of Civil Procedure* §338, “an action upon a liability created by
15 statute” applies and the limitation is three years. In either case Plaintiff started its action within the
16 prescribed period and has therefore not waived its rights based on time limitations.

17 Waiver may occur when Plaintiff fails to include a claim in a complaint, but generally causes of
18 action may be added with the permission of the court at any time. Since Plaintiff is not claiming any
19 additional claims this defense does not apply.

20 Therefore, Defendant’s affirmative defense of waiver by Plaintiff is meritless and should be
21 barred as a matter of law.

22 **10. There is no factual or legal basis for the defense asserted by Defendant that**
23 **Plaintiff’s claims are barred under the doctrine of preemption.**

24 The *CAN SPAM Act* is a statute enacted by the federal legislature and therefore can only be
25 preempted by another Federally created statute. No such law has been created. *California Business*
26 *and Professions Code* §17529.5 is specifically preserved by the *CAN SPAM Act*. Therefore none of
27 Plaintiff’s causes of action are preempted.

28 The Supremacy Clause invalidates state laws that interfere with, or are contrary to, federal law.
U.S. Const. Art. 6, cl. 2; *Engine Mfrs. Ass'n v. South Coast Air Quality Management Dist.*, 498 F.3d

1 1031 at 1039 (9th Cir., 2007). “Federal preemption occurs when: (1) Congress enacts a statute that
2 explicitly preempts state law; (2) state law actually conflicts with federal law; or (3) federal law
3 occupies a legislative field to such an extent that it is reasonable to conclude that Congress left no room
4 for state regulation in that field.” *Ibid.*

5 Since no federal law has been enacted to reverse or change the *CAN SPAM Act*, it has not been
6 affected, and Defendant’s defense is meritless.

7 The *CAN SPAM Act* specifically preempts State laws pertaining to emails in 15 *USC*
8 7707(b)(1). However, the same section specifically preserves State laws that deal with fraud or
9 computer crime. 15 *USC* 7707(b)(2)(B). *California Business and Professions Code* §17529.5
10 specifically deals with fraudulent or misleading advertisements and makes the advertiser liable for the
11 advertisement. Since the California code falls within the saving paragraph of the *CAN SPAM Act* it
12 cannot be preempted by the Act.

13 Therefore, Defendant’s affirmative defense of preemption is meritless and should be barred.

14 **11. There is no factual dispute that Plaintiff is a provider of Internet Access as**
15 **defined in 15 USC 7706(g)(1). There is no factual dispute that Plaintiff is a**
16 **provider of Email Services within the definition of California Business and**
Professions Code §17529.5.

17 Plaintiff is an IAP and ESP as defined in the applicable statutes. 15 *USC* 7706(g)(1) provides
18 standing for a provider of Internet access services adversely affected to bring an a claim under the *CAN*
19 *SPAM Act*. An Internet Access Service is defined in 15 *USC* 7702(11) has having the “meaning given
20 that term in section 231(e)(4) of Title 47.” 47 *USC* 231(e)(4) defines Internet Access Service as:

21 The term “Internet access service” means a service that enables users to access
22 content, information, electronic mail, or other services offered over the Internet,
23 and may also include access to proprietary content, information, and other
services as part of a package of services offered to consumers. Such term does not
include telecommunications services.

24 *California Business and Professions Code* §17529.5(b)(1)(A)(II) provides standing for an
25 “electronic mail service provider” to bring an action under the statute. *California Business and*
26 *Professions Code* §17529.1(h) defines an electronic mail service provider as:

27 means any person, including an Internet service provider, that is an intermediary
28 in sending or receiving electronic mail or that provides to end users of the
electronic mail service the ability to send or receive electronic mail.

1 As described above in the Statement of facts, **ASIS** has been in business as an Internet Access
2 Provider since 1995, and had just over 1,000 customers for both access services and email in 2005, when
3 the events of this case occurred. **ASIS** has provided invoices to customers for provision of those
4 services. **ASIS** has provided invoices from vendors for facilities used in provision of those services.
5 Nella White, President of **ASIS**, has declared that **ASIS** is an IAP and ESP. Defendant has provided no
6 evidence to the contrary.

7 Therefore, the issue of whether **ASIS** is an IAP and ESP has been established, and this fact
8 should be ordered established by the court.

9 **12. There is no factual dispute that the emails at issue were sent or transmitted**
10 **to ASIS email accounts and that they were received by ASIS.**

11 Plaintiff has declared the emails were sent or transmitted to its email server. The emails all
12 contain sent to email addresses of “@asis.com.” Defendant has provided no evidence that the emails
13 were not sent or transmitted to Plaintiff **ASIS**.

14 15 *USC* 7704(a) makes it illegal to transmit to a protected computer emails in violation of the
15 section. 15 *USC* 7706(g) provides standing for an IAP that is adversely affected by a violation of 15
16 *USC* 7704(a)(1)–(5). Therefore, if the emails were sent to **ASIS**, that fact provides standing for **ASIS** to
17 bring this action and direct proof that the emails were transmitted to **ASIS**’ protected computer.
18 Protected computer is defined as the meaning given in “section 1030(e)(2)(B) of Title 18.” 18 *USC*
19 1030(e)(2)(B) defines protected computer as a computer “which is used in interstate or foreign
20 commerce or communication.” Since **ASIS**’ service is used to access the internet and send email
21 anywhere in the world it is used in interstate and foreign commerce and communications.

22 Defendant can provide no evidence that the emails were not sent to **ASIS**’ protected computer.
23 Therefore, the issue of whether the emails were sent or transmitted to **ASIS** has been established, and
24 this fact should be ordered established by the court.

25 **13. There is no factual dispute that the subject emails contain false header**
26 **information.**

27 The subject emails contain false header information and this fact should be established.

28 15 *USC* 7704(a)(1) makes it a violation to send any email that contains false or materially
misleading header information to a protected computer. False header is defined, in part, if it fails to

1 accurately identify the sender because:

2 if it fails to identify accurately a protected computer used to initiate the message
3 because the person initiating the message knowingly uses another protected
4 computer to relay or retransmit the message for purposes of disguising its origin.
5 15 *USC* 7704(a)(1)(C).

6 Further 15 *USC* 7704(a)(6) defines “materially” in respect to false or misleading header
7 information as the alteration or concealment of header information in a manner that impairs an
8 investigator from identifying the sender.

9 Plaintiff has provided evidence that the sending IP addresses and the sending domain names do
10 not match, as discussed above in ¶4 of the Statement of Facts above. In fact, most of the sending IP
11 addresses are not even from the correct country of origin for the sending domain names. Therefore,
12 either the sending IP addresses have been altered or the sending domain addresses are not the actual
13 senders. Even if the sending IP addresses were altered by use of an anonymous email process then they
14 were altered in a manner that conceals the true sender from an investigator, and are therefore in
15 violation. 15 *USC* 7704(a)(1).

16 Further, the way the emails were sent, in time bursts and alphabetical order, indicates the emails
17 were sent in a coordinated fashion. See ¶4 of Statement of Facts above. This type of coordination can
18 only occur when there is a controlling computer coordinating the sending of the emails. This is a clear
19 indication that the emails were sent using a botnet of hijacked computers. Sending emails in this manner
20 without the permission of the computer owners is a direct violation of 15 *USC* 7704(a)(1)(A) and (b)(3).

21 Therefore, Plaintiff has established that the email headers were false in violation of 15 *USC*
22 7704(a)(1), and this fact should be ordered established by the court.

23 **14. There is no factual dispute that the emails contain false or misleading subject
24 lines.**

25 The subject emails are commercial electronic mail messages and contain false subject lines in
26 violation of 15 *USC* 7704(a)(2) and *California Business and Professions Code* §17529.5(a)(3). (See
27 Statement of Facts)

28 15 *USC* 7704(a)(2) states that it is a violation for any person to send a commercial electronic
mail message:

1 if such person has actual knowledge, or knowledge fairly implied on the basis of
2 objective circumstances, that a subject heading of the message would be likely to
3 mislead a recipient, acting reasonably under the circumstances, about a material
4 fact regarding the contents or subject matter of the message (consistent with the
5 criteria used in enforcement of section 45 of this title).

6 15 *USC* 45 empowers the FTC to prevent unlawful and unfair competitive practices including
7 false advertisements. The FTC has issued several regulations, incorporated in the Code of Federal
8 Regulations, that define and govern the area of false advertisements. 16 *CFR* 251 defines how words
9 such as “free” or offers of free products may be used in advertisements. 16 *CFR* 238, defines the use of
10 an advertisement offer to bait a consumer and then switch to another offer.

11 Plaintiff has provided exhaustive evidence that the subject lines in the subject emails are clearly
12 intended to trick the recipient, by providing clearly false information such as “mortgage approved”, into
13 opening the email and then offering a service to get mortgage refinance offers. See ¶4 in the Statement
14 of Facts above.

15 Therefore, Plaintiff has established that the subject emails contain false subject lines in violation
16 of 15 *USC* 7704(a)(2), and this fact should be ordered established by the court.

17 **15. There is no factual dispute that the emails do not contain a valid unsubscribe**
18 **option and a physical opt-out address in violation of 15 *USC* 7704(a)(5).**

19 The subject emails do not contain valid unsubscribe options or a physical opt-out address and are
20 in violation of 15 *USC* 7704(a)(5).

21 15 *USC* 7704(a)(5)(A)(ii) makes it a violation to send a commercial electronic mail message that
22 does not contain a “clear and conspicuous” opportunity to decline to receive further emails. 15 *USC*
23 7704(a)(5)(A)(iii) makes it unlawful to send a commercial electronic mail message that does not contain
24 the valid physical postal address of the sender.

25 As discussed in ¶6 of the Statement of Facts above, only 131 of 12,756 emails contain anything
26 that resembles a valid unsubscribe opportunity. Not one of the emails contains a valid physical postal
27 address of the sender. Therefore the emails are in violation of 15 *USC* 7704(a)(5).

28 Therefore, Plaintiff has established that the subject emails do not contain valid unsubscribe
opportunities or the physical address of the sender, and this fact should be ordered established by the
court.

1 **II. CONCLUSION**

2 Plaintiff respectfully requests the Court summarily adjudicate the foregoing issues in Plaintiff's
3 favor.

4 **SINGLETON LAW GROUP**

5 Dated: January 16, 2008

6 /s/ Jason K. Singleton
7 Jason K. Singleton,
8 Richard E. Grabowski, Attorneys for Plaintiff,
9 **ASIS INTERNET SERVICES**