

**Exhibit U**

**(Conditionally Filed Under Seal)**

# Exhibit V

1 Jason K. Singleton, State Bar #166170  
lawgroup@sbcglobal.net

2 Richard E. Grabowski, State Bar #236207  
rgrabows@pacbell.net

3 SINGLETON LAW GROUP  
4 611 "L" Street, Suite A  
Eureka, CA 95501  
5 (707) 441-1177  
FAX 441-1533

6 Attorneys for Plaintiff, ASIS INTERNET SERVICES

7  
8 UNITED STATES DISTRICT COURT  
9 NORTHERN DISTRICT OF CALIFORNIA

10 ASIS INTERNET SERVICES, a California) Case No. C-05-5124 JCS  
11 corporation, )  
12 Plaintiff, ) PLAINTIFFS' EXPERT WITNESS  
13 vs. ) DISCLOSURE OF JEFFREY POSLUNS  
14 )  
15 OPTIN GLOBAL, INC., a Delaware) Corporation, also dba Vision Media)  
16 USA Lenders Network, )  
17 USA Lenders, and USA Debt )  
Consolidation Service; et al., )  
Defendants. )

18 Comes now Plaintiff, who hereby provides an expert witness disclosure in conformance  
19 with Rule 26 (a)(2) of the Federal Rules of Civil Procedure.

20 DISCLOSURE

21 1. Plaintiff discloses JEFFREY POSLUNS as Plaintiff's expert in the above  
22 captioned matter. JEFFREY POSLUNS will testify as to the Internet, email services, SPAM,  
23 SPAM abuse by Defendants, and violations of the **CAN SPAM Act** and **California Business**  
24 **and Professions Code** §17529.5.

25 2. JEFFREY POSLUNS' opinion will be based upon his inspection of documents  
26 and files, education, training, technical analysis of the evidence at issue, Federal and State  
27 court cases, Federal and State statutes, and research of various publicly available information  
28 sources related to SPAM. Defendant has been provided copies of the documents reviewed,

1 already has those documents, or was the original source of the documents.

2 3. JEFFREY POSLUNS' qualifications are set forth in full in his Curriculum Vitae  
3 attached to as Exhibit "A".

4 4. SecuritySage Overdrive Inc. (where JEFFREY POSLUNS is an executive and  
5 co-founder) charges \$200.00 per hour for time spent by JEFFREY POSLUNS consulting,  
6 \$200.00 per hour for trial and deposition testimony, and \$100 per hour for time spent by  
7 research assistants.

8 5. JEFFREY POSLUNS has testified as an expert in two other cases in the last five  
9 years. Jeffrey Posluns was disclosed by Ritchie Phillips dba R&D Computers as its expert  
10 witness in December of 2006 in the case of *Phillips v. Netblue, C-05-4401 SC*, this case  
11 settled in 2007 without going to trial. Jeffrey Posluns offered written testimony in the Phillips v.  
12 Netblue case in the plaintiff's expert disclosure. Jeffrey Posluns also provided oral testimony  
13 in an oral deposition taken by the defendant, Netblue. Jeffrey Posluns was disclosed by  
14 Timothy J. Walton of Walton & Rosses LLP in the case of *Daniel L. Balsam v. Expedite*  
15 *Media Group Inc.* where he offered written testimony. This case has not yet gone to trial.

## 16 REPORT

17 1. Attached hereto and incorporated herein by reference as Exhibit "A" is a true and  
18 correct copy of my Curriculum Vitae. I have the training, education, and experience set forth  
19 therein.

### 20 I. QUALIFICATIONS

21 I, Jeffrey Posluns, am an expert in Internet security and Internet electronic mail. I have  
22 over a decade of experience in the management of security and technology companies, with  
23 expertise in risk management, security tools and techniques, anti-spam technologies, intrusion  
24 detection/prevention, and incident response. Having founded, co-founded, and invested in  
25 several e-commerce and security initiatives, I have served in the capacity of President/CEO,  
26 CTO, and CIO.

27 I am the currently the Chief Information Officer of SecuritySage Overdrive, Inc., 4480  
28 Cote de Liesse, Suite #390, Montreal, Quebec, Canada, H4N2R1, (888) 776-4987.

1 **II. SCOPE OF ENGAGEMENT**

2 I have been retained to offer oral and/or written testimony about the electronic mail sent  
3 to Plaintiff's protected computer and Plaintiff's business. Specifically, I will testify about  
4 whether Plaintiff is an Internet Access Provider, provides email services, if the electronic mail  
5 Plaintiff received can be categorized as SPAM, and the degree of knowledge that Defendants  
6 had regarding the spamming activities.

7 My testimony will include my personal and professional knowledge of Internet  
8 technology, Internet security, Internet Mail technology, the SPAM industry/business, and  
9 compliance with California and federal law.

10 My testimony will also include my analysis of the emails at issue and other pertinent  
11 evidence provided for my review.

12 **III. INFORMATION REVIEWED**

13 To prepare my opinions, I considered the following:

- 14 A. Industry and legal definitions regarding the Internet, the CAN SPAM Act, and  
15 California Business and Professions Code §17529.5. (Attached hereto as Exhibit  
16 B).
- 17 B. Information industry, Internet, electronic mail, and SPAM concepts. (Attached  
18 hereto as Exhibit C).
- 19 C. 12,576 emails provided by Plaintiff and attorney received by ASIS from October  
20 2005 through January of 2006.
- 21 D. Plaintiff's Second Amended Complaint (hereafter "SAC").
- 22 E. Defendants' Answer to the SAC.
- 23 F. Plaintiff's Supplement to the SAC.
- 24 G. Plaintiff's Interrogatories and Requests for Production and Defendant's  
25 Responses.
- 26 H. Production of internal documents and emails produced by Azoogle.
- 27 I. Depositions with exhibits of:
  - 28 a. Nella White;

- 1           b.     Don Mathis;
- 2           c.     Alex Baydin;
- 3           d.     Ryan McVey;
- 4           e.     Richard Okin;
- 5           f.     Alexander Zhardanovsky;
- 6           g.     John White;
- 7           h.     Marvin Hernandez;
- 8           i.     Sally Then;
- 9           j.     Joe Spieser
- 10          k.     Julian Mossanen
- 11          J.     Studies prepared by Carl Scoles and provided under Plaintiff's Response to
- 12             Court Ordered Interrogatories.
- 13          K.     Study prepared by Josh Mohland and provided under Plaintiff's Response to
- 14             Court Ordered Interrogatories.
- 15          L.     Diagrams of various email and Internet processes, to be used at trial. (Attached
- 16             hereto as Exhibit D).
- 17          M.     RFC 2821, The Simple Mail Transfer Protocol.
- 18          N.     RFC 2822, Internet Message Format, published in 2001, also known as 822bis.
- 19             Replaced RFC 822 (1992) and RFC 1123 (1989) (Attached hereto as Exhibit E).
- 20          O.     Databases (RBLs and ROKSO) and publicly available information from
- 21             SPAMHAUS.
- 22          P.     Knowledge gained in acting as the technical editor for *Inside the SPAM Cartel*,
- 23             Syngress Publishing, October 2004, and other industry books and reports.
- 24          Q.     Bandwidth graphs and server configuration files provided by Nella White.
- 25             (Attached hereto as Exhibit F).
- 26          R.     FTC policy papers defining unfair and fraudulent competition: FTC GUIDE
- 27             CONCERNING USE OF THE WORD "FREE" AND SIMILAR
- 28             REPRESENTATIONS; Frequently Asked Advertising Questions: A Guide for

1 Small Business GENERAL ADVERTISING POLICIES; DOT COM  
2 DISCLOSURES; FTC POLICY STATEMENT ON UNFAIRNESS Appended to  
3 International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n);  
4 and FTC POLICY STATEMENT ON DECEPTION Appended to Cliffdale  
5 Associates, Inc., 103 F.T.C. 110, 174 (1984). (Attached hereto as Exhibit G).

6 **IV. SUMMARY OF OPINION**

7 Based on my understanding of the issues in the complaint and on the scope of this  
8 engagement, it is my opinion that the Defendants have failed to fully comply with the **CAN**  
9 **SPAM Act** and the **California Business and Professions Code** §17529.5. More particularly,  
10 my opinion includes the following:

11 A. **ASIS Internet Services, Inc. is an Internet Access Provider.** This opinion is  
12 based on:

- 13 a. The industry and legal definitions included in Exhibit B.
- 14 b. The concepts included in Exhibit C.
- 15 c. The ASIS vendor invoices provided by Plaintiff in its discovery  
16 disclosures.
- 17 d. Ownership of various domain names used to provide Internet and  
18 email service.
- 19 e. The 12,756 emails provided as part of Plaintiff's disclosure.
- 20 f. Bandwidth graphs and server configuration files provided by ASIS  
21 Internet Services.

22 Analysis:

23 Per a telephone discussion with Nella White of ASIS, ASIS has invoiced  
24 clients for Internet access services. Any company with clients to whom Internet  
25 access services are provided is an Internet access provider. ASIS has provided  
26 me with bandwidth graphs showing Internet utilization. This shows that ASIS is  
27 offering services to the Internet, making ASIS a provider of Internet services.

28 B. **ASIS is an email service provider.** This opinion is based on:

- a. The industry and legal definitions included in Exhibit B.
- b. The concepts included in Exhibit C.
- c. The vendor invoices provided by Plaintiff in its discovery disclosures.
- d. Ownership of various domain names used to provide Internet and email service.
- e. The 12,576 emails provided as part of Plaintiff's disclosure.
- f. Bandwidth graphs and server configuration files provided by ASIS.

Analysis:

Nella White of ASIS has provided me with a copy of the configuration of their mail server's anti-spam solution, and has verbally described the configuration of the email server that is used by ASIS customers. This shows that ASIS has an email server and is offering email services to its clients.

C. **The header information in the subject emails contained false and misleading information.** This opinion is based on:

- a. The industry and legal definitions included in Exhibit B.
- b. The concepts included in Exhibit C.
- c. Ownership of various domain names used to provide Internet and email service.
- d. The 12,756 provided as part of Plaintiff's disclosure and my analysis of those emails.
- e. The declarations of Carl Scoles and Josh Mohland containing analysis of the subject emails.
- f. My analysis of the subject emails.

Analysis:

In many of the emails, the sending IP address' reverse DNS information does not match the sender's email domain name nor does it match the domain name with which the sending host identifies itself. While this may occur in some

1 virtual hosting environments, many of the IP addresses belonged to the  
2 computers of individuals making use of a standard internet provider to access the  
3 internet. This indicates that the header information is false. This false information  
4 was generated at the time that the emails were sent using a program that  
5 specifically generates false header information while sending emails.

6 An investigation of the IP addresses in the email headers indicates that  
7 the emails were sent or relayed from individual computers making use of  
8 standard internet service providers for access to the internet. In order to send out  
9 the subject emails, these computers would have been infected with malicious  
10 code (commonly referred to as a virus, Trojan, or botnet application) and made  
11 members of a botnet. The use of a botnet conceals the true sender of the emails  
12 from the receiving ISP. (See Josh Mohland's Study).

13 **D. The subject lines of the emails sent to ASIS's protected computer were**  
14 **misleading.**

- 15 a. The industry and legal definitions included in Exhibit B.
- 16 b. The concepts included in Exhibit C.
- 17 c. The 12,576 emails provided as part of Plaintiff's disclosure and my  
18 analysis of those emails.
- 19 d. The declarations of Carl Scoles containing analysis of the subject  
20 emails.
- 21 e. FTC policy papers defining unfair and fraudulent competition.  
22 Exhibit G.
- 23 f. My analysis of the subject emails.

24 **Analysis:**

25 9,163 of the emails contain subject lines that claim the recipient has either  
26 been approved or pre-approved for a mortgage. These emails contain a link that  
27 offers to get brokers to call the recipient, after providing confidential information.  
28 These subject lines are therefore misleading or completely false and intended to

1 get the recipient to open the emails, as the sender has no previous knowledge of  
2 the recipient.

3 42 of the emails contain subject lines that claim that there is a pre-existing  
4 application on file. Since the emails are trying to get a recipient to fill out a form  
5 with their personal information that will be used to get refinance quotes, this  
6 cannot be a truthful statement.

7 36 of the emails contain subject lines that describe places of interest, such  
8 as "Vacation homes w/oceanview for L;e:ss." Since this has nothing to do with  
9 the offer in the email it is a misleading subject line intended to get the recipient to  
10 open the email.

11 352 of the emails contain subject lines that have nothing to do with  
12 mortgages or refinance, such as "Message subject" or "Re: Office Admin."

13 19 of the emails contain subject lines that refer to making money, such as  
14 "Make \$..."

15 23 of the emails contain subject lines that appear to be asserting a prior  
16 relationship, such as "More Information needed" or "Urgent matter."

17 78 of the emails contain subject lines that claim that there is important  
18 information, such as "Important Email. Details inside." This subject line is clearly  
19 intended to trick the recipient into opening the email.

20 24 of the emails contain no subject line at all.

21 The contents of the emails offer loans for various amounts at different  
22 interest rates. The landing pages that the URLs contained in the emails send the  
23 recipient to are advertisements to get loan advisors to call after submitting  
24 personal financial information. Since the email subject lines do not describe that  
25 these are really advertisements intended to induce the recipient into submitting  
26 personal financial information in order to get mortgage brokers to call them, they  
27 are misleading subject lines. Therefore, 9737 emails contain false or misleading  
28 subject lines.

1 E. **The emails were sent on behalf of Azoogie.** This opinion is based on:

- 2 a. The industry and legal definitions included in Exhibit B.
- 3 b. The concepts included in Exhibit C.
- 4 c. The 12,576 emails provided as part of Plaintiff's disclosure and my
- 5 analysis of a sample of those emails, including:
- 6 i. The subject lines of the emails;
- 7 ii. The body text of the emails;
- 8 iii. The target sites and domain names of URLs
- 9 contained in the emails;
- 10 d. The declarations of Carl Scoles and Josh Mohland containing
- 11 analysis of the subject emails.
- 12 e. Azoogie's discovery disclosures.
- 13 f. ASIS's discovery disclosures.
- 14 g. Quicken Loans and Aegis discovery disclosures.

15 Analysis:

16 An analysis of the IP addresses for the landing pages of the URLs

17 contained in the subject emails clearly shows the landing pages are connected.

18 The URL in 5,569 of the subject emails open an identical page, or a page

19 containing identical images to those seen at WUMORT.NET – the page that

20 Nella White used to enter the "Bruce Wolf" lead in October of 2005. Of the 5,569

21 emails, 4,217 linked to an identical page as that seen by Nella White in October

22 2005. The other 1,352 emails linked to pages containing at least 6 of the same

23 image files used in the wumort.net web page. When a comparison of the IP

24 addresses of the URL links was made, a connection became apparent between

25 the 92 web domains in 11,418 of the subject emails.

26 The probability is extremely remote that landing pages from different

27 emails will contain the same images and be housed on a network of the same IP

28 addresses and not be from the same source. There are some four trillion

possible IP addresses on the Internet, making coincidences relating to IP

1 addresses very unlikely.

2 Analysis of the email characteristics ties the emails closely together. The  
3 fact that the emails appear to be a pre-programmed set of forms with different  
4 elements substituted into the form indicates that the emails were from the same  
5 source.

6 The use of a botnet and the characteristics of how they were used (emails  
7 sent in alphabetical order from different botnet members every few minutes) adds  
8 additional evidence that the emails were sent by the same source.

9 The "Bruce Wolf" lead was filled in on the exact same page to which over  
10 1500 of the emails directed the recipient (i.e. wumort.net and wumort.com). The  
11 "Bruce Wolf" lead was delivered to Quicken Loans by Azoogole as part of  
12 Azoogole's "lowrateadvisors.com" advertising campaign. (See the actual lead  
13 sheet provided by Quicken Loans as QL-0116 identifying the lead source as  
14 "LowRateAdvisors.com"). This ties all of those 1500 plus emails directly to the  
15 Azoogole advertising campaign.

16 Images and a near duplicate landing page were discovered on Azoogole's  
17 servers. The similarity of the Azoogole server images and the  
18 LowRateAdvisors.com web page to the actual pages viewed by Nella White in  
19 October 2005, and their similarity to the other email landing pages, tie the entire  
20 set of emails to Azoogole's advertising campaign, LowRateAdvisors.com.

21 **F. White labeling, as used by Azoogole, hides the true identity of the advertiser**  
22 **from the consumer. Azoogole attempted to remove itself from directly**  
23 **taking part in the spamming operation, though directly benefited from the**  
24 **spam that was sent.** This opinion is based on:

- 25 a. The industry and legal definitions included in Exhibit B.  
26 b. The concepts included in Exhibit C.  
27 c. Emails provided in the Lendance subpoena response discussing the  
28 use of "white labeling".

- 1 d. Emails provided in the Angelfire subpoena response discussing
- 2 “white labeling” and the use of redirects.
- 3 e. Emails to and from SPAMHAUS discussing the use of redirectors by
- 4 Azoogle affiliates. AZ SP-000046.
- 5 f. The declarations of Carl Scoles and Josh Mohland containing
- 6 analysis of the subject emails.

7 Analysis:

8 The communications produced by Lendance and Angelfire, as well as  
9 Julian Mossanen’s deposition clearly indicate that Azoogle was promoting the use  
10 of “white labeling” by their third party contractors and affiliates. In white labeling,  
11 the actual entity offering or advertising the product or service is not identified to  
12 the consumer. White labeling hide’s the true identity of the actual entity offering  
13 or advertising the product or service. (See a definition of “White Label” in Exhibit  
14 B Definitions).

15 SPAMHAUS warned Azoogle in February of 2005 that the reason they  
16 could not identify which affiliates were spamming from the complaints they were  
17 receiving, was because of the use of redirectors in the affiliate landing pages.  
18 The use of redirectors effectively hid the identity of Azoogle, the real advertiser,  
19 from the consumer and made it difficult for Azoogle to identify the spammer.  
20 Azoogle AZ SP 000046.

21 It is clear that Azoogle was using “White Labeling” (having a third party use  
22 a site not connected with Azoogle, and then forwarding the leads generated from  
23 that site directly to Azoogle) and that SPAMHAUS told Azoogle that this is why  
24 Azoogle could not detect the use of SPAM by their partners. While this may be a  
25 valid form of product distribution in the normal advertising world, in internet  
26 marketing, it only disguises the true identity of the advertiser. This allows the  
27 advertiser to appear remote from the spamming operation while still benefiting  
28 directly from the spam.

1 Neither the email nor the landing page identified Azoogole as the advertiser;  
2 however the "Bruce Wolf" lead was delivered to Azoogole by their third party  
3 contractor, Seamless Media. The landing page used to collect the data is almost  
4 identical to the Azoogole LowRateAdvisors.com page discovered on Azoogole's  
5 servers. The only real difference between the web pages is the information that  
6 identifies Azoogole as the advertiser. The source code used to display the  
7 websites is almost exactly the same. This is a typical scenario for a white label  
8 web page, where the advertiser has hired a partner to advertise their service  
9 without identifying the actual entity offering or advertising the product or service.  
10 The fact that Azoogole received the lead indicates that they were the advertiser  
11 providing the inducement. Moreover, Mr. Mathis testified Azoogole's third party  
12 lead vendors were under contract to sell the leads generated under the I.O. only  
13 to Azoogole.

14 **G. The emails were sent using a botnet – a series of compromised protected**  
15 **computers.** This opinion is based on:

- 16 a. The industry and legal definitions included in Exhibit B.  
17 b. The concepts included in Exhibit C.  
18 c. The declarations of Carl Scoles and Josh Mohland containing  
19 analysis of the subject emails.  
20 d. My analysis of the emails received by ASIS.com

21 Analysis:

22 The study performed by Josh Mohland shows that the emails were sent  
23 using an alphabetical list of ASIS email accounts. These emails were sent in  
24 bursts every few minutes from different computers. The only way for emails to  
25 be sent in exact alphabetical order from different computers in a short period of  
26 time is if the computers had their lists of email recipients managed and/or  
27 provided from the same source. A botnet is a series of computers that have  
28 been taken over using malicious code (such as viruses, Trojans, or botnet

1 applications) and are under the control of a source which can be a single  
2 individual or computer, or any member of a group with access to the controlling  
3 mechanism. See a complete definition of botnets in Exhibit B Definitions. The  
4 computers used to send the emails were not SMTP mail servers. Analysis of the  
5 IP addresses of the sending computers indicates that they were consumer  
6 personal computers with normal consumer access to the internet (e.g. DSL,  
7 Cable, Dial-up). These computers appear to have been taken over by an  
8 unknown party in order to send the emails. It is typical for an individual to build a  
9 botnet, and then sell access to the botnet to spammers who will then use it to  
10 send bulk and/or SPAM email without revealing their identity. Therefore, the  
11 emails sent to ASIS.com were sent using a botnet of compromised computers  
12 without the permission of the computers' owners.

13 H. **Azoogle and it's affiliates/third party contractors have spammed a**  
14 **significant number of times in the past, and continue to do so. There is no**  
15 **apparent effort on the part of Azoogle to prevent third party contractors**  
16 **from spamming. Azoogle is aware that they had third party contractors**  
17 **who were spamming. Azoogle does not know the identity of the sub-**  
18 **affiliates of their affiliates and third party vendors. This implies that**  
19 **Azoogle consciously avoids knowledge of the spam activities, or chooses**  
20 **to ignore the knowledge that they do have.** This opinion is based on:

- 21 a. The industry and legal definitions included in Exhibit B.
- 22 b. The concepts included in Exhibit C.
- 23 c. Depositions of Azoogle managers.
- 24 d. Results of Subpoenas sent to third party vendors.
- 25 e. Searches in Newsgroups: news.admin.net-abuse for the domains of
- 26 the senders and sending hosts.
- 27 f. SPAMHAUS ROKSO listings.

28 ///

1 Analysis:

2 Azoogle had good notice that their affiliates were using SPAM to send  
3 their advertisements. Azoogle was listed on ROKSO until April of 2006 primarily  
4 because of their inability to control their affiliates. See the emails from  
5 SPAMHAUS in AZ – SP00001 – 50.

6 Several of the third party contractors used by Azoogle were also listed on  
7 ROKSO. OptinRealBig owned by Scott Richter is considered one of the top  
8 spamming operations of all time and has been involved in multiple SPAM suits.  
9 OptinRealBig was not terminated by Azoogle until March of 2007. See Mathis  
10 Deposition pg. 343. JDR Media and Tranzact Media were also affiliates or third  
11 party vendors of Azoogle. See Zhardanovsky Deposition Pg. 156 - 157. JDR  
12 Media is still listed on the SPAMHAUS ROKSO list as a “(l)ong running spam  
13 operation”, see ROK3859. Tranzact Media is also still listed on ROKSO, see  
14 ROK4420.

15 Azoogle does not know where their affiliates or their third party vendors  
16 get their email lists. See Okin Deposition pg. 147. Azoogle has not audited any  
17 third part vendor’s email list. See Okin Deposition pg. 148.

18 Even though Azoogle has a suppression list and was provided  
19 suppression lists by the mortgage brokers they were dealing with, these lists  
20 were never provided to the third party vendors. McVey Deposition Pgs. 141 –  
21 145. These lists are only used to check sales leads prior to providing them to  
22 mortgage brokers.

23 Azoogle does nothing to test its third party vendors. Most of the subpoena  
24 responses from the third party vendors state that they had little or no contact with  
25 Azoogle beyond the purchase order or advertising insertion order they received.  
26 No third party vendor received any policies, procedures or training regarding  
27 CAN SPAM from Azoogle. No discussions were held between Azoogle and their  
28 third party vendors concerning avoiding CAN SPAM violations. The Advertising

1 insertion order used by Azoogole as a contract with their third party vendors does  
2 not contain any reference to avoiding violations of the CAN SPAM Act. The only  
3 reference in the Advertising Insertion Orders regarding SPAM is a prohibition  
4 against using Azoogole's suppression list for spamming.

5 I. **Azoogole was doing nothing to vet their affiliates/third party contractors and**  
6 **was doing nothing to check on spamming activities. Azoogole was**  
7 **consciously avoiding knowing that their third party contractors and**  
8 **affiliates were spamming.** This opinion is based on:

- 9 a. The industry and legal definitions included in Exhibit B.
- 10 b. The concepts included in Exhibit C.
- 11 c. Depositions of Azoogole managers.
- 12 d. Results of Subpoenas sent to third party vendors.
- 13 e. Searches in Newsgroups: news.admin.net-abuse for the domains  
14 of the senders and sending hosts.
- 15 f. SPAMHAUS ROKSO listings.
- 16 g. Savvis Communication Corp., an internet service provider providing  
17 internet access to Azoogole in late 2004, terminated Azoogole's  
18 service because of multiple SPAM complaints. Savvis Subpoena  
19 response. Alex Zhardanovshy stated that after being terminated by  
20 Savvis, Azoogole did nothing to change their spam policing policies.  
21 Zhardanovsky Deposition Pg. 109 L. 23 – Pg. 110 L. 5.
- 22 h. Azoogole was listed on the SPAMHAUS ROKSO list in 2004 and  
23 2005. Azoogole was removed from the list in April 2006. Both Alex  
24 Zhardanovsky and Joe Spieser, the founders of Azoogole,  
25 communicated through email with SPAMHAUS representatives as  
26 to why Azoogole was on the ROKSO list and what they needed to do  
27 to get off of the list. Primarily Azoogole was failing to manage their  
28 affiliates and could not even identify the affiliates who were

1 spamming. See the Azoogole produced emails between Azoogole  
2 and SPAMHAUS AZ – SP00001 - 50.

3 i. Statements made by the Azoogole’s COO and CIO at deposition:

4 i. Statement from Deposition of Azoogole Chief Operating  
5 Officer Don Mathis representing Azoogole as their  
6 Person Most Knowledgeable Pg. 24 and 25:

7 10 Q Who was tasked with the compliance  
8 11 functions before November of 2005?

9 12 A The -- the answer is there was no  
10 13 one individual. It was consistent with the  
11 14 company being a fairly early stage start-up  
12 15 handled by a number of people on a -- from a  
13 16 time-to-time basis. The compliance effort  
14 17 was driven primarily by technology algorithms  
15 18 that had been written. The --

16 19 Q Say that last part again, because I  
17 20 didn't --

18 21 A So the compliance effort prior to  
19 22 October -- or November of 2005 consisted  
20 23 primarily of a set of technology algorithms  
21 24 and the oversight of the chief technology  
22 25 officer, the business people in the company

23 25

24 1 Mathis  
25 2 who were directly related to the driving of  
26 3 traffic.

27 ii. Statement from Deposition of Azoogole Chief Information  
28 Officer Richard Steven Okin Pg. 43:

1 3 Q Getting back to this technology  
2 4 algorithm, can you tell me how many of the  
3 5 three features that we have just discussed  
4 6 would serve any purpose in a spam policing  
5 7 policy in Azoogole’s affiliate network?

6 ...  
7 16 A I can’t think of how they would help  
8 17 off the top of my head.

Mr. Okin states on pages 79 and 80 of his deposition  
that he has never conceived of or been asked to think of any

1 way of policing to prevent SPAM by affiliates or third party  
2 contractors.

3 These statements clearly indicate that the COO  
4 thought there were only two methods of CAN SPAM  
5 compliance during October and November of 2005: the  
6 technology algorithm; and the oversight of the Chief  
7 Technology Officer. However, the CIO stated there was  
8 nothing in the technology algorithms that dealt with SPAM  
9 policing and that he has never been approached on the  
10 subject.

- 11 j. The policies and procedures regarding spamming applied to  
12 affiliates were not applied to third party vendors. While Azoog  
13 checks on the tax ID of an affiliate and compares it with their  
14 physical address to verify that they have presented their real  
15 identity, they do not apply this action to third party vendors. Mathis  
16 Deposition.
- 17 k. No formal auditing or tracking mechanism for spam complaints was  
18 in place in 2005 or early 2006, based upon the deposition testimony  
19 of the Azoog managers.
- 20 l. Alex Zhardanovsky stated that there was no job function at Azoog  
21 “to go out and catch spam”. Zhardanovsky Deposition Pg. 18 line  
22 10 – 11. Mr. Zhardanovsky stated that there was a two or three  
23 strike rule that was used to terminate a publisher (a publisher is a  
24 name used by Azoog for their affiliates). The two strike rule was  
25 used if an ISP complained and the three strike rule was used if  
26 consumers complained. Zhardanovsky Deposition Pg. 20 line 15 –  
27 21. This is clearly a reactive policy. The other procedures Mr.  
28 Zhardanovsky’s opined that were used to identify spammers and

1 prevent spamming, such as seeding lists and checking ROKSO,  
2 were not supported by the other witnesses from Azoogole.  
3 Apparently Mr. Zhardanovsky thought the integrity assurance  
4 program (also called the compliance program) was started in early  
5 2005 when Don Mathis and Charlie came on board. Zhardanovsky  
6 deposition pg. 9. However, Don Mathis started with Azoogole in late  
7 September of 2005 (Mathis Deposition Pg. 224 L. 24 – 25) and  
8 Charles Noviczech was hired by Mr. Mathis in March of 2006 to  
9 start the integrity program. Mathis Deposition Pg. 234 L 10 - 12.  
10 Mr. Mathis stated that his primary activity, when he started, was  
11 overseeing the Azoogoleads technology, his title was Senior Vice  
12 President of Technology and Operations. Mathis Deposition Pg. 6  
13 and 13. Therefore, neither individual could have played a  
14 significant part in SPAM compliance in October and November of  
15 2005. Mr. Mathis also stated that the integrity  
16 assurance/compliance program was not started until March of  
17 2006. Mathis Deposition Pg. 234 L. 10 – 12.

18 m. Mr. Alex Baydin, Azoogole's Vice President and General Manager of  
19 Verticals, stated that he had received no training on the CAN SPAM  
20 Act or SPAM prevention policies at Azoogole. Baydin deposition Pg.  
21 149 L. 20 – 23. Mr. Baydin also stated that he did not know if  
22 anything was done to determine if third party vendors were violating  
23 the CAN SPAM Act other than what was done by the compliance  
24 department. Baydin deposition Pg. 167 - 168. Since the integrity  
25 assurance/compliance program did not start until March of 2006  
26 when Charles Noviczech was hired it could not have had any  
27 impact during late 2005 and early 2006. Mathis Deposition Pg. 234  
28 L. 10 – 12.

1 n. Azoogle left open to the general public a deactivated web page,  
2 LowRateAdvisors.com, which has been used repeatedly without  
3 authorization by Azoogle, by spammers. This occurred in the within  
4 case, and in several others. Several witnesses testified there is no  
5 business purpose to be served by Azoogle in leaving a deactivated  
6 web page open to the general public. Moreover, the allegedly  
7 unauthorized use of the lowrateadvisor.com site in the incarnation  
8 lowrateadvisors.net, had an href link back to a lowrateadvisors.com  
9 site on Azoogle's server.

10 Analysis:

11 Azoogle had good notice that they had a spamming problem based on  
12 their termination by Savvis and the SPAMHAUS listing. Azoogle did nothing  
13 beyond their two/three strike policy to police the activities of their affiliates until  
14 March of 2006. There is nothing to show that Azoogle did or has ever done  
15 anything to police their third party contractors. The testimony of the CIO indicates  
16 that the algorithms relied on by Mr. Mathis did not do anything to police spam.  
17 Although all the managers said some one else was responsible for CAN SPAM  
18 compliance, the people identified had no responsibility and took no action to  
19 police SPAM. Therefore, Azoogle was consciously avoiding knowing that their  
20 third party contractors and affiliates were using SPAM to generate mortgage  
21 leads.

22 J. **Azoogle has claimed that a spammer must have stolen their**  
23 **LowRateAdvisors.com images and html code, and then used those to**  
24 **generate leads back to Azoogle. These leads directly benefited Azoogle,**  
25 **and there is no reasonable explanation as to how and why any entity other**  
26 **than Azoogle itself would benefit from stealing site images and html code,**  
27 **creating a new page with that same code, and sending leads back to**  
28 **Azoogle. This implies that Azoogle's theory that their images and html**

1 **code was stolen is faulty.** This opinion is based on:

- 2 a. Industry Knowledge.
- 3 b. Logic and deductive reasoning.
- 4 c. Knowledge gained in acting as the technical editor for ***Inside the***
- 5 ***SPAM Cartel***, Syngress Publishing, October 2004, and other
- 6 industry books and reports
- 7 d. Azoogole has not provided any evidence or reasonable explanation
- 8 as to why a spammer would have stolen their images and html
- 9 code.

10 Analysis:

11 It is not technologically feasible to steal the executable code portion of the

12 page in question that stores and/or submits the data gathered on the web forms

13 to a backend storage mechanism without extreme effort or skill. Considering that

14 the data submitted by Nella White made its way to Azoogole, the entity that put up

15 the web site in question must have either been granted access to this executable

16 code portion, or must have compromised the standard security mechanisms in

17 place on a valid PHP-enabled and Azoogole-managed web site in order to steal

18 the backend executable source code. If the entity that put up the web site in

19 question did so in order to benefit themselves, said entity must have been

20 grossly negligent and/or incompetent (unreasonable considering the skills

21 necessary to perform said code theft) considering that said entity did not validate

22 the flow of form data such that it would have gone to a storage mechanism

23 owned and/or managed by said entity instead of to Azoogole. The theoretical

24 stealing of images, html code, and backend executable code did not benefit an

25 entity other than Azoogole itself as the leads generated from such went to

26 Azoogole.

27 Marvin Hernandez testified that the Azoogole Lead Agents software

28 recorded the URL of the landing page of the third party vendor from which each

1 lead was generated. The Quicken loan produced document lists the "Bruce Wolf"  
2 lead as coming from the "lowrateadvisors.com" web site. A reasonable inference  
3 may thus be drawn that Azoogle knew, or should have known, that its third party  
4 vendor was using the web site on which Nella White filled in the Bruce Wolf lead  
5 to generate leads for sale to Azoogle. Azoogle only needed to view that site and  
6 the domain's WHOIS registration information to determine the purposes for which  
7 that site was being used.

8  
9 **V. COMPENSATION**

10 SecuritySage Overdrive Inc (where JEFFREY POSLUNS is an executive and co-  
11 founder) charges \$200.00 per hour for time spent by JEFFREY POSLUNS consulting, \$200.00  
12 per hour for trial and deposition testimony, and \$100 per hour for time spent by research  
13 assistants.

14  
15 I reserve the right to revise and correct this report.

16  
17  
18  
19 Dated: September 7, 2007

20  
21  
22  
23  
24  
25  
26  
27  
28  
  
Jeffrey Posluns

**PROOF OF SERVICE**

I declare that I am a resident of the State of California, over the age of eighteen years, and not a party to the within action. My business address is, Singleton Law Group, 611 "L" Street, Suite "A", Eureka, CA 95501.

On September 10, 2007, I served the following document:

**PLAINTIFF'S EXPERT DISCLOSURE**

on the parties listed below as follows:

**Henry M. Burgoyne, III**  
**KRONENBERGER BURGOYNE LLP**  
150 Post Street, Suite 520  
San Francisco, CA 94108  
(hank@kronenbergerlaw.com)  
cc: Jeff Rosenfeld (jeff@kronenbergerlaw.com)  
Peter Touschner (paralegal@kronenberger.com)

**By facsimile machine (FAX)** by personally transmitting a true copy thereof via an electronic facsimile machine to # (415) 955-1158

**By first class mail** by placing a true copy thereof in a sealed envelope with postage thereon fully prepaid and placing the envelope in the firm's daily mail processing center for mailing in the United States mail at Eureka, California.

**By EMAIL** to the address(es) listed above

**By personal service** by causing to be personally delivered a true copy thereof to the address(es) listed herein at the location listed herein.

**By Federal Express, UPS, or overnight mail**

**(State)** I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

**(Federal)** I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on September 10, 2007, at Eureka, California.

/s/ Roberta Alliston  
Roberta Alliston