

1 **Jason K. Singleton, State Bar #166170**  
lawgroup@sbcglobal.net  
2 **Richard E. Grabowski, State Bar #236207**  
rgrabows@pacbell.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, R&D COMPUTERS**

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

10 **RITCHIE PHILLIPS, dba R&D** ) **Case No. C-05-4401 SC**  
11 **COMPUTERS,** )  
12 **Plaintiff,** ) **DECLARATION AND SUPPLEMENTAL**  
13 **vs.** ) **DISCLOSURE OF JEFFREY POSLUNS**  
14 **NETBLUE, INC., formerly known as** )  
15 **YFDIRECT, INC., also doing business as** )  
16 **MARKETSURVEYGROUP.COM, also dba** )  
17 **EASYEZSTREET.COM, also dba** )  
18 **MINGLYCOMP.INFO, also dba** )  
19 **EVERYFREEGIFT.COM, KENNETH CHAN,** )  
20 **aka KENNETH CHEN, SCOTT REWICK,** )  
21 **DEREK PILCH, FREDRICK HARMAN, and** )  
22 **DOES ONE through FIFTY, inclusive,** )  
23 **Defendants.** )

24 I, Jeffrey Posluns, declare as follows:

25 The following is a Supplemental Declaration to Plaintiff's Expert Witness Disclosure and  
26 Declaration of Jeffrey Posluns served on Defendants and contains:

27 **OPINIONS (IDENTICAL TO ORIGINAL DOCUMENT) WITH SUMMARIES AND**  
28 **SUPPORTING EXPLANATIONS**

**A. R&D Computers is an Internet Access Provider.**

Per a telephone discussion with Ritchie Phillips of R&D Computers and Richard

1 E. Grabowski of Singleton Law Group, R&D Computers has invoiced clients for Internet  
2 access services. Any company with clients to whom Internet access services are  
3 provided is an Internet access provider. Ritchie Phillips of R&D Computers has  
4 provided me with bandwidth graphs showing Internet utilization. This shows that R&D  
5 Computers is offering services to the Internet, making R&D Computers a provider of  
6 Internet services.

7 B. **R&D Computers is an email service provider.**

8 Ritchie Phillips of R&D Computers has provided me with a copy of the  
9 configuration of their mail server's anti-spam solution, and has verbally described the  
10 configuration of the email server that is used by R&D Computers customers. This shows  
11 that R&D Computers has an email server and is offering email services to its clients.

12 C. **The emails were sent on behalf of Netblue.**

13 The emails reviewed by me personally and those reviewed by SSO personnel  
14 contained advertisements for products that are marketed by NetBlue. The links in the  
15 bodies of the emails were to servers used by NetBlue. The emails for which the sending  
16 organization was easily determined were sent by known affiliates of NetBlue. This is  
17 sufficient evidence to formulate the opinion that the emails were sent on behalf of  
18 NetBlue.

19 D. **The true sender of the subject emails cannot be determined or can only be**  
20 **determined by extraordinary means.**

21 The sender name and sender email address in the emails do not reference a real  
22 person or real company. The whois information on the domains are obfuscated using  
23 privacy services or options to hide the real owners of the domains names. The reverse  
24 IP lookup of the IP addresses of the sending servers indicate Internet hosting providers  
25 and not the organization making use of the servers. The contact information on web  
26 sites referenced by the emails do not contain telephone numbers which can be related  
27 to an individual or company using reverse telephone lookup methods. In order to  
28 determine the true senders of the emails, valid contact information must be found for

1 one of the items listed above, or the cooperation of a hosting company or domain  
2 registrar must be obtained.

3 E. **The emails reviewed contained false header information.**

4 The emails were missing information in the headers that would, in standard email  
5 communications, provide information about the message and/or sender and/or sending  
6 server. The servers used to send the emails either did not create or removed any such  
7 headers not required to deliver the emails. Emails sent by individuals using standard  
8 email programs contain headers providing information about the software and/or system  
9 used to send the email. These headers were missing from the emails. Emails sent by  
10 individuals or sent automatically by servers using industry standard practices will  
11 contain a Message ID. This is a series of seemingly random letters and/or numbers that  
12 will allow system administrators (or other persons with access to the sending server's  
13 logs) to look up information about a particular email by referencing the message ID.  
14 Message IDs were not provided by all the sending servers.

15 Netblue states that both Cogent and Spamhaus have informed them that there  
16 are affiliates who use forged (false) headers.

17 Each of the facts above denote false header information.

18 F. **The subject emails contain misleading subject lines:**

19 The information contained in the subject lines of emails offer free products or  
20 money, and do not indicate any requirements or reference any terms and conditions.  
21 The bodies of emails however offer free products for performing various tasks, such as  
22 clicking a link which then takes the reader to web pages that contain terms and  
23 conditions. The subject lines are thus misleading the reader into believing that he/she  
24 will receive something for free whereas that is not in fact the case.

25 G. **The emails were sent from mass email generation tools on hosts (servers) that**  
26 **are configured similarly to known spam sending servers. This implies that the**  
27 **servers sending the emails are spam sending servers, as there is no valid reason**  
28 **for them to be configured such under generally accepted business practices for**

1           **sending emails.**

2           There is no valid business or personal reason for mail servers and sending hosts  
3 to forge or falsify headers in a standard business or personal email process. Forging or  
4 falsifying headers is a common tactic used by spammers in their attempts to bypass  
5 spam filters and have recipients read otherwise unwanted emails. The source IP  
6 addresses of sending servers of emails have also been matched to hosts that were  
7 previously known to send spam. This was done via RBL lookups. This is sufficient  
8 evidence to formulate the opinion that the sending hosts were servers that are  
9 configured to send spam.

10 H.       **There is no practical business reason why commercial emails would have their**  
11 **source information removed unless the party responsible for the sending server**  
12 **is engaged in spamming activities.**

13           This is a logical deduction based on industry standard practices for email servers  
14 and email client software. My experience in managing, configuring, and working with  
15 email servers, anti-spam solutions, and email service providers over the past ten (10)  
16 years supports this opinion.

17 I.       **NetBlue affiliates have spammed a significant number of times in the past, and**  
18 **continue to do so. While some efforts to deal with spam complaints have been**  
19 **taken, there is no apparent effort on the part of NetBlue to prevent affiliates from**  
20 **spamming.**

21           The number of spam complaints as shown in disclosures provided by Netblue  
22 indicates that affiliates have been sending spam at least as far back as the  
23 implementation of the abuse management system. Some Netblue affiliates have  
24 reputations as spammers, and at least three have been sued for spam related activities.  
25 There are multiple listings in the Spamhaus SBL for Netblue affiliates, and Netblue was  
26 almost listed in ROKSO per Netblue disclosure NET6778. The lack of activities to  
27 prevent illegal spamming by affiliates on the part of Netblue such as attempts to enforce  
28 a compliance policy and/or reviewing affiliates and sub-affiliates prior to signing them

1 supports the opinion that Netblue has not made any efforts to prevent affiliates from  
2 spamming illegally or otherwise. That Netblue affiliates have spammed in the past and  
3 continue to do so is fact.

4 J. **NetBlue is aware that they have a significant number of affiliates who are**  
5 **spamming. Netblue is aware that their sub-affiliates are spammers who have**  
6 **reputations of spamming, and may already be listed on ROKSO. This implies that**  
7 **Netblue consciously avoids knowledge of the spam activities, or chooses to**  
8 **ignore the knowledge that they do have.**

9 Netblue disclosures show many communications indicating that Netblue affiliates  
10 and sub-affiliates send spam, that Netblue will allows persons with ROKSO listings  
11 (such as Bill Wagoner) to become sub-affiliates, and that Netblue personnel are actively  
12 involved in attempting to remove blacklist listings related to spam issues. This indicates  
13 that at least some Netblue personnel are fully aware of the spam related issues. The  
14 lack of activities on the part of Netblue (see opinion I above) to prevent illegal spamming  
15 and their claims to not be involved with spamming indicates that either some of Netblue  
16 senior management are not being made aware of the business practices of the  
17 company, a conscious decision on the part of Netblue personnel to prevent knowledge  
18 of spam issues from reaching others, or that Netblue personnel choose to ignore the  
19 knowledge that they do have unless spam issues are affecting their revenues.

20 K. **Netblue is aware that they hire / bring on new affiliates and sub-affiliates who are**  
21 **spammers, and make no apparent efforts to prevent such.**

22 Netblue disclosures clearly show that Netblue is aware that their affiliates and  
23 sub-affiliates are spammers, and that new affiliates and sub-affiliates are not reviewed  
24 to ensure that they are not spammers. Netblue has taken the position that they are not  
25 responsible for the activities of their sub-affiliates, though they clearly benefit from the  
26 activities of said sub-affiliates. This position is an apparent attempt to justify their lack of  
27 efforts to prevent known spammers and spamming organizations from becoming sub-  
28 affiliates.

1 L. **Netblue chooses to defer dealing with spam problems and avoids responsibility**  
2 **for their spam (affiliate and sub-affiliate) issues rather than be proactive and deal**  
3 **with them directly. Only when a spam issue impacts revenue do they take**  
4 **immediate action.**

5 Per Netblue disclosures, when there is a spam related issue that could affect  
6 Netblue's internet services (email delivery or web site availability), Netblue changes  
7 service providers rather than deal with the source of the issues. This is a clear case of  
8 avoiding taking responsibility for their actions or lack of actions. Netblue internal emails  
9 back up this opinion by showing that Netblue is aware that they have affiliates with  
10 spam issues that could affect Netblue, and that Netblue attempts to distance  
11 themselves or make changes to obfuscate their relationship with these affiliates.

12 M. **Netblue consciously deals with black lists in an attempt to keep the most revenue**  
13 **coming in, and considers revenue as more important than ethics or legal**  
14 **compliance. Netblue takes the path of the least effort (and least cost) rather than**  
15 **put in the effort required to deal with their spam problems.**

16 Netblue disclosures show that Netblue provides affiliates (or sub-affiliates) with  
17 guidance on how to appease Spamhaus to have a blacklist entry removed, not how to  
18 deal with the issue that caused the blacklist entry to be added in the first place. Netblue  
19 is not consistent in their practices of terminating policy offenders, to the point that  
20 "\_\_\_\_\_" one of NetBlue's named affiliates (name omitted per Protective Order) – a  
21 known spamming organization with a ROKSO listing is allowed to continue as an  
22 affiliate. Affiliates who do not generate very high revenues are terminated, whereas  
23 Netblue prefers that affiliates who do generate high revenues deal with their blacklist  
24 listings so that they will not have to be terminated, and an account that generates high  
25 margins was deactivated to appease Spamhaus and subsequently reactivated to continue  
26 generating revenues. While this may be a sound business decision from the financial  
27 perspective, it is clear that Netblue values revenues over ethics and compliance.


28 ///

1 N. Netblue claims to have the intent to keep better track of sub-affiliates, though  
2 they have not put any noticeable efforts into doing so. This implies that they are  
3 consciously avoiding taking any actions that will generate active proof of  
4 particular sub-affiliate spamming.

5 In order to keep track of sub-affiliates, it would be necessary to make  
6 technological changes to the Netblue system such as the URLs for landing pages.  
7 Netblue disclosure NET7370 dated February 14, 2006 shows the intent to do so, though  
8 as of December 2006 in the deposition of Peter Adams, no such mechanism had been  
9 put in place. Per discussions with experts in the field of web development, the efforts to  
10 implement such a system would take approximately one man week to develop, then an  
11 additional week to implement, test, and distribute information to affiliates. Even if these  
12 activities took two or three times the time frames estimated, they would have been  
13 implemented well before December 2006. This indicates that Netblue has not put efforts  
14 into implementing such a system.

15 I declare under penalty of perjury under the laws of the United States of America that  
16 the foregoing is true and correct.

17  
18 Dated: January 12, 2007

19   
20 \_\_\_\_\_  
21 JEFFREY POSLUNS