4 law.co.il

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK by ELIOT SPITZER, Attorney General of the State of New York,

Petitioners,

-against-

SYNERGY6, INC., d/b/a SYNERGY6.COM, AMERICAN-GIVEAWAYS.COM, and HOTFREESAMPLES.COM, JUSTIN CHAMPION, OPTINREALBIG.COM, LLC, d/b/a OPTINREALBIG.COM, SCOTT RICHTER, DELTA SEVEN COMMUNICATIONS, LLC, PAUL BOES, and DENNY COLE,

Respondents.

NOTICE OF VERIFIED PETITION

Index No. _____

PLEASE TAKE NOTICE, that upon the annexed Verifed Petition, verified on December 18, 2003, and the accompanying Affirmation of Assistant Attorney General Stephen Kline, executed December 17, 2003, with exhibits annexed, Petitioners will move this Court at the Motion Support Office Court Room, Room 130 of 60 Centre Street, New York, New York, on the 28th day of January, 2004, at 9:30 o'clock in the forenoon or as soon thereafter as counsel may be heard, for an Order and Judgment:

WHEREFORE, Petitioners request that this court grant relief pursuant to Executive Law § 63(12) and General Business Law §§ 349 and 350 against the Respondents by issuing an Order and Judgment as follows:

i. Permanently enjoining Respondents from further engaging in any of the fraudulent, deceptive, and illegal acts and practices described in the Verified Petition, including through their agents;

ii. Permanently enjoining Respondents and any agents acting on their behalf from using false or misleading information in the header information on commercial emails;

iii. Permanently enjoining Respondents and any agents acting on their behalf from falsifying the transmission path of any commercial email;

iv. Requiring Respondents to disgorge any money or other benefits derived from Respondents' fraudulent and illegal activities;

v. Permanently enjoining any of the Respondents from doing business in, or directed to, the State of New York until such time as such Respondent posts a bond of One Hundred Thousand Dollars ($100,000) with a corporate surety from a company licensed to do business in this State, payable in favor of the People of the State of New York for the benefit of any future consumer who may be injured by any of such Respondent's practices or by such Respondent going out of business;

vi. Directing Respondents to notify Petitioners of any change of address within five days of such change, and to notify Petitioners of their creation or operation of any business or web site offering merchandise or services, within five days of such creation or operation. For the purposes of this Verified Petition, a Respondent creates a business when, alone or in conjunction with others, if Respondent owns more than five percent of such business, forms a new business or web site offering merchandise or services;

vii. Directing each Respondent to provide a certified accounting, indicating (a) the

total number of emails sent for each of the campaigns described herein; (b) the content, including header lines (and/or methodology by which such header lines were chosen), of each email campaign described in (a); and (c) the total number of responsive emails from, and shipments to, consumers located in, or apparently located in, New York.

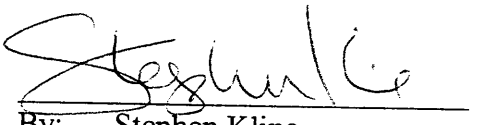
viii. Directing that a money judgment in civil penalties pursuant to GBL §350-d be entered against each Respondents in favor of the State of New York, based upon the sum of Five Hundred Dollars ($500) per each instance of a deceptive or unlawful act or practice alleged or discovered during the pendency of this litigation (including without limitation acts based on information ascertained based upon a certified accounting, as described in (vii)), above;

ix. Directing that a money judgment be entered against Respondents in favor of Petitioners in the sum of Two Thousand Dollars ($2,000) in costs against Respondents, pursuant to C.P.L.R. §8303(a)(6); and

ix. Granting Petitioners such other and further relief as this Court finds just and proper.

Date: December 17, 2003
New York, New York

ELIOT SPITZER
ATTORNEY GENERAL
OF THE STATE OF NEW YORK



By: Stephen Kline
Assistant Attorney General
Internet Bureau
Attorney for Petitioner
120 Broadway, 3rd Floor
New York, New York 10271
Stephen.Kline@oag.state.ny.us
(212) 416-6250

KENNETH M. DREIFACH
Assistant Attorney General in Charge
Internet Bureau

STEPHEN KLINE
Assistant Attorney General
Of Counsel

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK by ELIOT SPITZER, Attorney General of the State of New York,

Petitioners,

-against-

SYNERGY6, INC., d/b/a SYNERGY6.COM, AMERICAN-GIVEAWAYS.COM, and HOTFREESAMPLES.COM, JUSTIN CHAMPION, OPTINREALBIG.COM, LLC, d/b/a OPTINREALBIG.COM, SCOTT RICHTER, DELTA SEVEN COMMUNICATIONS, LLC, PAUL BOES, and DENNY COLE,

Respondents.

VERIFIED PETITION

Index No. _____

The People of the State of New York, by Eliot Spitzer, Attorney General of the State of New York, allege upon information and belief that:

INTRODUCTION

1. Respondents are spammers, people who are responsible for sending untold amounts of unsolicited commercial emails ("spam") containing false headers and routing information and deceptive subject lines. They hide behind fake identities, fake email addresses, and utilized hundreds of insecure servers worldwide in order to prevent consumers from identifying them as the senders of unwanted junk email.

2. Petitioners bring this summary proceeding (a) to enjoin Respondents from using false or

misleading information in the headers of commercial emails; (b) to enjoin Respondents from causing the source of their commercial emails to be falsely identified; (c) to enjoin Respondents from using false or misleading subject lines in their commercial emails; (d) to require Respondents to disgorge any profits derived from their illegal activities; (e) to require Respondents, prior to continuing their business activities, to post a bond to protect future consumers; and (f) to recover costs and penalties as authorized by statute, and such other relief as requested herein.

3. Respondents have sent a torrent of unsolicited commercial email messages ("spam"), all of which either attempted to hide Respondents' identity by falsifying the identity of the emails' sender or source, or contained false or misleading subject lines. Each such instance of Respondents' illegal, fraudulent, and deceptive conduct is set forth in greater detail in the accompanying Affirmation of Assistant Attorney General Stephen Kline dated December 17, 2003, with attached exhibits ("Kline Aff.").

JURISDICTION AND PARTIES

4. Petitioners are the People of the State of New York, by their attorney, Eliot Spitzer, Attorney General of the State of New York. Petitioners have offices in the County of New York, located at 120 Broadway, New York, New York.

5. Petitioners bring this Special Proceeding pursuant to Executive Law § 63(12), alleging underlying persistent and repeated fraudulent and illegal conduct pursuant to General Business Law ("GBL") §§ 349 and 350 (deceptive business practices and false advertising).

6. GBL § 349 empowers the Attorney General to seek injunctive relief and restitution when any person or entity has engaged in deceptive acts or practices in the conduct of any business.

GBL § 350-d empowers the Attorney General to seek civil penalties in the amount of $500.00 for each violation of GBL § 350, the false advertising statute, and GBL § 349, the deceptive practices statute. In addition, Executive Law §§ 63(12) and 63(15) empower the Attorney General to seek injunctive relief, restitution, damages, and costs when any person or business entity has engaged in or otherwise demonstrated repeated fraudulent or illegal acts in the transaction of business.

7. Prelitigation notice as provided for in GBL § 349 and § 350-c has been given, by certified mail delivered on five or more days notice to Respondents. *See* Kline Aff. ¶ 37.

8. Respondent Synergy6, Inc. ("Synergy6") is a corporation organized under the laws of Delaware, with its principal place of business at 336 West 37th Street, 14th Floor, New York, New York, 10018-4212. Synergy6 is an online marketing company with a web site (www.Synergy6.com) that promotes its marketing activities including email marketing, and co-registration – the practice of generating leads, subscriptions, or memberships concurrent with another registration process. *See* Kline Aff. ¶ 6.

9. Respondent Justin Champion is, and was at all times relevant to this Petition, the President of Synergy6, and Mr. Champion directed and controlled the activities of Synergy6. *See* Kline Aff. ¶ 7.

10. OptInRealBig, LLC ("OptInRealBig") is a limited liability company organized under the laws of Nevada, with its principal place of business at 1333 W. 120th Avenue, Suite 101, Westminster, Colorado, 80234. OptInRealBig is an email marketing company with a web site (www.OptInRealBig.com) that promotes its work as an email marketing company. *See* Kline Aff. ¶ 8.

11. Respondent Scott Richter is the President of OptInRealBig and has directed and controlled the activities of OptInRealBig, including the day-to-day activities involving many aspects of the relationships with and between other Respondents. *See* Kline Aff. ¶ 9.

12. Respondent Delta Seven Communications, LLC, is a limited liability company formed under the laws of Texas, and at all times relevant to this Petition, its principal place of business was in Plano, Texas. *See* Kline Aff. ¶ 10.

13. Respondent Paul Boes, of Bothell, Washington, is an email marketer who, at all times relevant to this Petition was doing business as "Delta Seven Communications" in Plano, Texas. *See* Kline Aff. ¶ 10. On August 7, 2003, Boes filed a Voluntary Petition for Bankruptcy in the Eastern District of Texas. This action is brought as a police power action, seeking to enjoin conduct harmful to consumers. *See* Kline Aff. ¶ 11.

14. Respondent Denny Cole, of Dallas, Texas, was at all times relevant to this Petition an email marketer working with Boes and was doing business as "Delta Seven Communications" in Plano, Texas. *See* Kline Aff. ¶ 12.

THE BUSINESS MODEL OF SYNERGY6 AND ITS AFFILIATES

15. To generate lists of consumers to whom it will send commercial emails in the future, Synergy6 pays other email marketers, or "affiliates," including Respondent OptInRealBig, to send emails promoting Synergy6's co-registration web sites, American-Giveaways.com and HotFreeSamples.com. These co-registration web sites offer "free" products to consumers in return for the consumer registering to receive more commercial emails. OptInRealBig, in turn, also hires affiliates, including Respondents Delta Seven, Boes and Cole, to send a portion of its commercial emails. Synergy6 pays its affiliates a commission based on the number of

registrations the affiliate's emails generate. OptInRealBig passes on a portion of that commission to the affiliate responsible for the registration. *See* Kline Aff. ¶ 13, 14. Richter and OptInRealBig act as agents of Synergy6; Delta Seven, Boes, and Cole, in turn, act as agents of Richter, OptInRealBig, and Synergy6. As to the acts alleged herein, each such agent was acting within the course and scope of such agency.

16. Through coding symbols embedded in each email, Synergy6 is able to track which affiliates drive consumers to their web sites. Synergy6 has assigned Richter and OptInRealBig the affiliate code "CD32." OptInRealBig has assigned Boes and Cole, in turn, the affiliate code "wsb." *See* Kline Aff. ¶¶ 14, 19.

THE BUSINESS MODEL AT WORK: ONE MONTH OF SPAM

17. Respondents' relationships with one another have been mutually beneficial: during the one month period between May 13, 2003 and June 13, 2003, Delta Seven, Boes, and Cole sent millions of emails for OptInRealBig and Synergy6, generating more than 20,000 registrations for Synergy6 and thousands of dollars in income for OptInRealBig and themselves alike. *See* Kline Aff. ¶ 15.

18. Of the millions of emails Respondents sent, more than 8,000 of them were sent to Hotmail "spam traps," between May 13, 2003 and June 13, 2003. These "traps" are email accounts owned and maintained by Microsoft for the specific purpose of collecting commercial spam email. These 8,779 emails were provided by Microsoft to the Attorney General's Office and form the basis for this Petition. *See* Kline Aff. ¶ 16.

RESPONDENTS USED FALSE IDENTITIES, FALSE EMAIL ADDRESSES, DECEPTIVE SUBJECT LINES, AND FALSE SOURCE INFORMATION IN ORDER TO HIDE WHO WAS SENDING THEIR EMAILS

19. During the relevant period, Respondents sent 8,779 emails containing fraudulent and deceptive identifiers and subject lines to the trap accounts. These emails contained more than 40,000 instances of fraud in all. This total, representing only those emails sent to Hotmail spam traps, represents a minuscule portion of the millions of fruadulent emails Respondents sent overall. The below paragraphs describe the multifarious ways in which Respondents hid their identities, in an attempt to evade consumers detection, complaints, and filtering efforts. *See* Kline Aff. ¶¶ 16-33.

A. False Sender Identities

20. In 7,599 of Respondents' emails, Respondents used false sender identities to deceive consumers. The sender identity of an email is one of the first pieces of information consumers see when their email in-boxes are opened. That identity is the name listed under the "From:" column in a typical email in-box; it immediately follows "From:" in an opened email. These 7,599 emails employed any of the following false identification methods:

- 5,153 of these emails falsely identified the sender as the recipient's user name (with underscores and numbers removed);
- 1,515 of these emails falsely identified the sender by employing the user name from the corresponding false email address at any one of 100 domains, i.e., the unique names which identify Internet web sites, none of which is registered to Respondents;
- 269 of these emails falsely identified the sender as "Confirmations"; and

- 662 of these emails falsely identified the sender as one of the following eight other companies: AOL, Bigfoot, Lycos, United Online, Earthlink, Yahoo, Hotmail, and Input Output Marketing, Inc.

See Kline Aff. ¶¶ 21, 22.

B. False Sender Email Addresses

21. Respondents also falsely identified their own email address – many times claiming that the email came from the recipient's own email address. Of the 8,779 emails Respondents sent to Hotmail spam traps, every single one of them falsely identified the sender's email address as any one of 7,030 different email addresses.

- 7,264 of these emails falsely identified the sender's email address as one having the same user name as the recipient, but at one of the following eight domains: Bigfoot.com, AOL.com, Yahoo.com, Earthlink.net, Lycos.com, Untd.com, Stormnetwork.us, or Hotmail.com.
- 1,515 of these emails falsely identified the sender's email address as a random user name at any one of 100 domains, none of which is registered to Respondents.

Of the 8,779 emails, purportedly sent from 7,030 different addresses, 808 emails sent to Hotmail spam traps falsely indicate that they were sent from the same Hotmail spam trap email accounts. At least one consumer complained to Synergy6 and Richter that Respondents' email to him at his Hotmail account appeared to have been sent from his Earthlink.net email account. *See* Kline Aff. ¶¶ 23, 24.

C. False Email Server Names

22. Respondents also falsified the emails' headers (the code documenting the emails' transmission path) to make them appear to have been sent from servers corresponding to the false email addresses. In the 8,779 emails sent to the Hotmail spam traps, Respondents caused the email server from which the email originated to be falsely identified as one of 123 different email servers at 108 different domains.

- In 7,264 of these emails, the Respondents caused the email server from which the email originated to be falsely identified as any one of 23 servers at eight different domains: Bigfoot.com, AOL.com, Yahoo.com, Earthlink.net, Lycos.com, Untd.com, Stormnetwork.us, or Hotmail.com.
- In 1,515 of these 8,779 emails, the Respondents caused the email server from which the email originated to be falsely identified as any one of 100 servers at 100 different domains, none of which is registered to the respondents.

See Kline Aff. ¶¶ 25, 27.

D. False Originating Internet Protocol Addresses

23. Respondents further tried to hide their identity by routing their emails through servers all around the world that do not record the emails' transmission path. By routing each of the 8,779 emails through such servers, they caused each email to appear to have originated from one of 514 different servers, in 36 countries, on six continents – none of which belongs to Respondents. In reality, these IP addresses are registered to hundreds of different organizations including the Ministry of Finance in Kuwait, a grade school in Korea, an Internet Service Provider in Slovenia, and a small promotional products company in New York City. *See* Kline Aff. ¶¶ 28-31.

24. Among the servers through which Respondents routed the 8,779 emails caught in the spam traps was one belonging to Warjo Promotions in New York City, through whose server Respondents routed at least 77 emails. Warjo accesses the Internet, and leases the IP address 66.9.76.25, from IntelliSpace, Inc., also of New York City. Warjo does not send bulk commercial email, nor has it given permission or authority to anyone else to use its servers to send commercial email from its servers. Nonetheless, Respondents routed their emails through Warjo's server, in order to hide their own identities. Soon after Respondents started sending email to the spam traps, consumers complained to IntelliSpace mistakenly believing that one of its clients was sending fraudulent spam or allowing others to do so. *See* Kline Aff. ¶¶ 30, 31.

E. False and Deceptive Subject Lines

25. In addition to falsely identifying the source of their emails, Respondents also included false and deceptive subject lines in their emails, in an attempt to trick consumers into opening emails they otherwise would not. In many of the 8,779 emails, Respondents included false or deceptive subject lines pretending to reply to the recipient's prior email or claiming to be about another company:

- 3,596 of Respondents' emails falsely indicated that the email was a response to previous email by starting the subject line with the abbreviation "Re:," the standard indicator signifying that an email is a response to an email sent by the recipient, rather than unsolicited;
- 2,830 of Respondents' emails falsely indicated that the email was being passed along from another sender, by starting the subject line with the abbreviation "Fwd:," the standard indicator signifying that an email has been forwarded from a

previous recipient, rather than sent by the original author; and

- 1,039 of Respondents' emails falsely indicated they were sent from or on behalf of one of eight of the following companies: AOL, Bigfoot, Lycos, United Online, Earthlink, Yahoo, Hotmail, and Input Output Marketing, Inc.

See Kline Aff. ¶¶ 32, 33.

26. The more than 40,000 instances of deceptive conduct and forged headers reflect only the fraud committed in emails that happened to be sent to Hotmail spam traps. These emails represent only a minuscule fraction of the total amount of Respondents' fraudulent and deceptive conduct.

RESPONDENTS CONTINUED TO SEND FRAUDULENT EMAIL, AND TO ACCEPT ITS COMMERCIAL BENEFITS AFTER RECEIVING COMPLAINTS

27. Days after Respondents began flooding the Hotmail spam traps with their emails, consumers began sending complaints to both Synergy6 and Richter (which Synergy6 acknowledged were "scathing") detailing the fraud. Richter and Champion both had first hand knowledge of these complaints, personally discussing with each other and co-workers via email the "scathing complaints" they were receiving from consumers. Richter also discussed these complaints with Boes and Cole. Nonetheless, Respondents continued to send the fraudulent and deceptive spam for more than a month. *See* Kline Aff. ¶ 34.

28. All defendants received material economic and commercial benefits from this scheme. For instance, by the end of the month, the fraud-ridden emails generated 20,409 new leads to whom Synergy6 could (and presumably did) market. Synergy6 paid a commission for each lead generated to OptInRealBig, who, in turn, paid Boes and Cole through Delta Seven. *See* Kline

Aff. ¶ 34.

THE INDIVIDUAL DEFENDANTS ARE PERSONALLY LIABLE

29. Both Richter and Champion exercised control of their respective companies' material day-to-day corporate operations. Champion handled many aspects of his company's operations, including negotiating commissions, making arrangements to pay affiliates, and determining how much email affiliates should send. *See* Kline Aff. ¶ 34. Richter, likewise, handled technical problems, negotiated list acquisitions, sought payments from debtors, and responded to complaints from consumers and ISPs. *See id.* Boes and Cole personally sent the fraudulent emails, and were paid for their efforts. *See id.* As discussed supra, Richter and Champion had personal knowledge of the fraudulent emails sent by Boes and Cole within days of their delivery.

LARGE AMOUNTS OF FRAUDULENT SPAM WERE SENT TO RESIDENTS OF NEW YORK

30. On information and belief, Respondents have sent millions of their deceptive and unlawful emails to consumers. On information and belief, approximately five percent of these consumer recipients were New York residents. An accounting of the total emails sent, as well as the percentage of Synergy6's registrants who are New York residents would reveal an estimated total of emails containing violations. At a minimum, the Petitioners seek penalties in the amount of $500 per violation, based on the number of registrants from Respondents' deceptive and unlawful emails who are New York residents. *See* Kline Aff. ¶ 35.

FIRST CAUSE OF ACTION (DECEPTIVE ACTS AND PRACTICES)

31. GBL § 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any services in [New York]."

32. By engaging in the acts and practices described above, Respondents repeatedly and persistently have engaged in deceptive business practices in violation of GBL § 349.

33. Respondents' violations of GBL § 349 constitute repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SECOND CAUSE OF ACTION
(FALSE ADVERTISING)

34. GBL § 350 makes unlawful "false advertising in the conduct of any business, trade or commerce or in the furnishing of any service in [New York]."

35. By engaging in the acts and practices described above, Respondents repeatedly and persistently have engaged in false advertising in violation of GBL § 350.

36. Respondents' violations of GBL § 350 constitute repeated and persistent illegal conduct in violation of Executive Law § 63(12).

THIRD CAUSE OF ACTION
PURSUANT TO EXECUTIVE LAW
SECTION 63(12) -- FRAUD

37. Executive Law § 63(12) authorizes the Attorney General to seek injunctive relief whenever any person shall engage in repeated fraudulent or illegal acts or otherwise demonstrate persistent fraud or illegality in the carrying on, conducting, or transaction of business.

38. By engaging in the acts and practices described above, Respondents repeatedly and persistently have engaged in fraud in violation of Executive Law § 63(12).

WHEREFORE, Petitioners request that this court grant relief pursuant to Executive Law § 63(12) and General Business Law §§ 349 and 350 against the Respondents by issuing an Order and Judgment as follows:

i. Permanently enjoining Respondents from further engaging in any of the fraudulent, deceptive, and illegal acts and practices described in the Verified Petition, including through their agents;

ii. Permanently enjoining Respondents and any agents acting on their behalf from using false or misleading information in the header information on commercial emails;

iii. Permanently enjoining Respondents and any agents acting on their behalf from falsifying the transmission path of any commercial email;

iv. Requiring Respondents to disgorge any money or other benefits derived from Respondents' fraudulent and illegal activities;

v. Permanently enjoining any of the Respondents from doing business in, or directed to, the State of New York until such time as such Respondent posts a bond of One Hundred Thousand Dollars ($100,000) with a corporate surety from a company licensed to do business in this State, payable in favor of the People of the State of New York for the benefit of any future consumer who may be injured by any of such Respondent's practices or by such Respondent going out of business;

vi. Directing Respondents to notify Petitioners of any change of address within five days of such change, and to notify Petitioners of their creation or operation of any business or web site offering merchandise or services, within five days of such creation or operation. For the purposes of this Verified Petition, a Respondent creates a business when, alone or in conjunction with others, if Respondent owns more than five percent of such business, forms a new business or web site offering merchandise or services;

vii. Directing each Respondent to provide a certified accounting, indicating (a) the

total number of emails sent for each of the campaigns described herein; (b) the content, including header lines (and/or methodology by which such header lines were chosen), of each email campaign described in (a); and (c) the total number of responsive emails from, and shipments to, consumers located in, or apparently located in, New York.

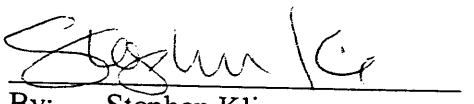
viii. Directing that a money judgment in civil penalties pursuant to GBL §350-d be entered against each Respondents in favor of the State of New York, based upon the sum of Five Hundred Dollars ($500) per each instance of a deceptive or unlawful act or practice alleged or discovered during the pendency of this litigation (including without limitation acts based on information ascertained based upon a certified accounting, as described in (vii)), above;

ix. Directing that a money judgment be entered against Respondents in favor of Petitioners in the sum of Two Thousand Dollars ($2,000) in costs against Respondents, pursuant to C.P.L.R. §8303(a)(6); and

ix. Granting Petitioners such other and further relief as this Court finds just and proper.

Date: December 17, 2003
New York, New York

ELIOT SPITZER
ATTORNEY GENERAL
OF THE STATE OF NEW YORK



By: Stephen Kline
Assistant Attorney General
Internet Bureau
Attorney for Petitioner
120 Broadway, 3rd Floor
New York, New York 10271
(212) 416-8433

KENNETH M. DREIFACH
Assistant Attorney General in Charge
Internet Bureau

STEPHEN KLINE
Assistant Attorney General
Of Counsel

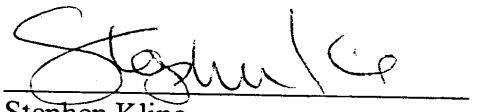
VERIFICATION

STATE OF NEW YORK)
) ss.:
COUNTY OF NEW YORK)

STEPHEN KLINE, being duly sworn, deposes and says: He is an Assistant Attorney General in the Office of Eliot Spitzer, Attorney General of the State of New York, and is duly authorized to make this verification.

He has read the foregoing Petition and knows the contents thereof, that the same is true to his own knowledge, except as to matters therein stated to be alleged on information and belief, and as to those matters he believes them to be true. The basis for this belief as to the matters alled on information and belief is the investigative files of the Internet Bureau.

The reason this verification is not made by Petitioners is that Petitioners are a body politic. The Attorney General is their statutory representative.



Stephen Kline

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK by ELIOT SPITZER, Attorney General of the State of New York,

Petitioners,

-against-

SYNERGY6, INC., d/b/a SYNERGY6.COM, AMERICAN-GIVEAWAYS.COM, and HOTFREESAMPLES.COM, JUSTIN CHAMPION, OPTINREALBIG.COM, LLC, d/b/a OPTINREALBIG.COM, SCOTT RICHTER, DELTA SEVEN COMMUNICATIONS, LLC, PAUL BOES, and DENNY COLE,

Respondents.

AFFIRMATION OF STEPHEN KLINE

Index No. _____

STEPHEN KLINE, an attorney admitted to practice before the courts of the State of New York, makes the following affirmation under penalty of perjury:

1. I am an Assistant Attorney General in the office of Eliot Spitzer, Attorney General of the State of New York, assigned to the Internet Bureau. I am familiar with the facts and circumstances of this proceeding.

2. The facts set forth in this affirmation are based upon information contained in the files of the Internet Bureau.

3. I submit this affirmation in support of the Attorney General's Verified Petition ("Petition") seeking an Order which, *inter alia*, enjoins Respondents and their agents from using false and deceptive identities and delivery practices in their commercial email campaigns, and

requires Respondents to post a performance bond and to pay civil penalties and costs for having engaged in such deceptive acts.

4. As set forth below, Respondents are professional email marketers who collectively send billions of commercial emails to consumers' in-boxes each week. These emails advertise a variety of products from free donuts to pornographic web sites. Sending huge volumes of commercial email, while annoying and burdensome to consumers, may not always be, in and of itself, illegal. However, the manner in which respondents have done so here – by deceiving consumers about the identity and source of their emails – is deceptive and unlawful. The emails' false sender identities and sources prevent consumers from identifying the respondents as the true senders of the emails, and hinder consumers' attempts to complain and/or block future mailings from Respondents.

5. In response to this repeated fraud and deception, Petitioners bring this summary proceeding (a) to enjoin Respondents and their agents from using false or misleading information in the headers of commercial emails; (b) to enjoin Respondents and their agents from falsely identifying the original source of their commercial emails; (c) to enjoin Respondents and their agents from using false or misleading subject lines in their commercial emails; (d) to require all Respondents to disgorge any profits derived from their illegal activities; (e) to require all Respondents prior to continuing their business activities, to post a bond to protect future consumers; and (f) to recover costs and penalties as authorized by statute, and such other relief as requested herein.

PARTIES AND BACKGROUND

A. Parties and Jurisdiction

6. Respondent Synergy6, Inc. ("Synergy6") is and was at all times relevant to the Petition, a corporation organized under the laws of Delaware. *See* Exh. 1 (Affidavit of Vanessa Ip, sworn to December 17, 2003 ["Ip Aff."] at ¶ 2); Exh. 2 (Certified Application for Authority of Synergy6, Inc.). Its principal place of business is 336 West 37th Street, New York, New York, 10018-4212. *See* Exh. 3 (Synergy6.com Homepage); Exh. 4 (Synergy6.com Contact Page); Exh. 1 (Ip Aff. at ¶ 3). Prior to some time in November 2003, Synergy6's principal place of business was 1250 Broadway, New York, New York, 10001. *See* Exh. 5 (Synergy6.com Registration Page). Synergy6 is an online marketing company with a web site (www.Synergy6.com) that promotes its marketing activities including email marketing, and co-registration – the practice of generating leads, subscriptions, or memberships concurrent with another registration process. *See* Exh. 1 (Ip Aff. at ¶¶ 3, 5, 6); Exh. 3 (Synergy6.com Homepage); Exh. 6 (American-Giveaways.com Homepage); Exh. 7 (American-Giveaways.com Registration Page); Exh. 8 (HotFreeSamples.com Homepage); Exh. 9 (HotFreeSamples.com Registration Page). Synergy6 also runs an affiliate marketing program called "Offerstream." *See* Exh. 1 (Ip Aff. at ¶ 7); Exh. 10 (Offerstream.com Homepage); Exh. 11 (Offerstream.com Registration Page).

7. Respondent Justin Champion ("Champion"), a resident of New York, is and was at all times relevant to this Petition the President of Synergy6. Champion directed and controlled the activities of Synergy6, and partook in email conversations involving many aspects of the relationship between Respondents. *See* Exh. 1 (Ip Aff. at ¶ 8); Exh. 12 (Synergy6 Emails Between Synergy6 Employees and OptInRealBig Employees).

8. Respondent OptInRealBig, LLC ("OptInRealBig") is a limited liability company organized under the laws of Nevada, with its principal place of business in Westminster, Colorado. *See* Exh. 1 (Ip Aff. at ¶¶ 9-11); Exh. 13 (Synergy6 Documents Re: "CD32" and Offerstream Terms and Conditions); Exh. 14 (Colorado Secretary of State Business Entities Search Results for "OptInRealBig.com, LLC"); Exh. 15 (Nevada Secretary of State Corporation Database Search Results for "OptInRealBig.com, LLC"). Its address is 1333 W. 120th Avenue, Suite 101, Westminster, Colorado, 80234. *See id.* OptInRealBig has a website (www.OptInRealBig.com) that promotes its work as an email marketing company. *See* Exh. 1 (Ip Aff. at ¶ 12); Exh. 16 (OptInRealBig.com Homepage); Exh. 17 (OptInRealBig.com Registration Page). OptInRealBig is an affiliate of Synergy6's Offerstream program, and OptInRealBig's affiliate code is "CD32." *See* Exh. 1 (Ip Aff. at ¶¶ 9, 13); Exh. 13 (Synergy6 Documents Re: "CD32" and Offerstream Terms and Conditions).

9. Respondent Scott Richter ("Richter"), a resident of Westminster, Colorado, is and was at all times relevant to this Petition part-owner and President of OptInRealBig, and directed and controlled the activities of OptInRealBig, including partaking in email conversations involving many aspects of the relationships between Respondents. *See* Exh. 1 (Ip Aff. at ¶¶ 8, 13-16, 18, 19, 24, 28, 29); Exh. 12 (Synergy6 Emails Between Synergy6 Employees and OptInRealBig Employees); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 39 (Consumer Complaint re: Respondents' Abuse of Consumer's Email Address); Exh. 46 (Complaints to Synergy6 and OptInRealBig re: Spam with Forged Headers); Exh. 47 (OptInRealBig Invoices and Synergy6 Checks for May and June 2003).

10. Respondent Delta Seven Communications, LLC ("Delta Seven"), is a limited liability company formed under the laws of Texas, and at all times relevant to this Petition, its principal place of business was in Plano, Texas. *See* Exh. 1 (Ip Aff. at ¶ 17); Exh. 19 (Texas Comptroller of Public Accounts Online Record for Delta Seven Communications, LLC). Delta Seven is an affiliate of OptInRealBig, with the affiliate code "wsb." See Exh. 1 (Ip. Aff. at ¶¶ 14-16, 18, 19); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests).

11. Respondent Paul Boes ("Boes"), a resident of Bothell, Washington, is and was at all times relevant to this Petition an email marketer. *See* Exh. 1 (Ip Aff. at ¶¶ 14, 15, 17, 19); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 19 (Texas Comptroller of Public Accounts Online Record for Delta Seven Communications, LLC). On August 7, 2003, Boes filed a Voluntary Petition for Bankruptcy in the Eastern District of Texas. *See* Exh. 20 (Boes Voluntary Petition for Bankruptcy). This action is brought as a police power action, in order to enjoin conduct harmful to consumers.

12. Respondent Denny Cole ("Cole"), a resident of Dallas, Texas, is and was at all times relevant to this Petition an email marketer. *See* Exh. 1 (Ip Aff. at ¶¶ 14, 15, 17, 19); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 19 (Texas Comptroller of Public Accounts Online Record for Delta Seven Communications, LLC).

B. Respondents' Activities

13. At all times relevant to this Petition, Synergy6 operated as both an email marketer and an

affiliate marketing program. As an email marketer, it would send commercial emails to consumers on behalf of others. Its affiliate marketing program, called "Offerstream," posts ads on a web site which other marketers, or affiliates, can then send to the affiliates' lists of consumers. Depending on the campaign, the affiliates are paid based on certain criteria, such as the number of sales or registrations generated.

14. To generate lists of consumers to whom it will send commercial emails, Synergy6 pays other email marketers, or "affiliates," including OptInRealBig, to send emails promoting Synergy6's co-registration web sites, American-Giveaways.com and HotFreeSamples.com. *See* Exh. 1 (Ip Aff. at ¶¶ 9, 13); Exh. 13 (Synergy6 Documents Re: "CD32" and Offerstream Terms and Conditions). OptInRealBig, in turn, also hires affiliates, including Boes and Cole, who in turn send a portion of this same set of commercial emails. *See* Exh. 1 (Ip Aff. at ¶¶ 14, 15, 18, 19); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests). By embedding coding symbols into each email, Synergy6 is able to track which of its affiliates drive consumers to its web sites. *See* Exh. 1 (Ip Aff. at ¶¶ 9, 13-15, 18-20, 29) Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 21 (Synergy6 Documents Re: Delta Seven Registrations and Payments to OptInRealBig).

15. For instance, as discussed below, during May and June 2003, Delta Seven, Boes, and Cole sent millions of emails on behalf of OptInRealBig and Synergy6. These emails directed consumers to the co-registration web sites where consumers would receive certain products in return for registering to receive more emails. These emails generated more than 20,000 registrations for Synergy6 and produced thousands of dollars of income for OptInRealBig as well

as for Delta Seven, Boes, and Cole. *See* Exh. 1 (Ip Aff. at ¶ 15, 20); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 21 (Synergy6 Documents Re: Delta Seven Registrations and Payments to OptInRealBig).

B. Summary of Violations

16. Between May 13, 2003 and June 13, 2003, Respondents sent more than 8,000 commercial emails to MSN Hotmail "spam traps." These "traps" are email accounts owned and maintained by Microsoft. Microsoft examines the emails received by these accounts as one of the methods it uses to determine whether incoming mail complies with the Terms of Use and Anti-Spam Policy for its MSN and MSN Hotmail services. The identity of these accounts is confidential, and the account names must remain confidential, so that spammers cannot avoid detection by removing the accounts' email addresses from their lists. *See* Exh. 22 (Affidavit of Jesse David Falk). Although these 8,779 emails were sent by a single advertiser, using only two affiliates, the emails falsely identified the sender by employing 2,990 fictitious names and 7,030 email accounts, at 105 different domains. The emails' headers also falsely identified the emails as having been sent from 123 different email servers. In addition, more than 5,000 of the emails contained deceptive subject lines. All 8,779 emails falsely appear to have been originally sent from 514 different servers in 35 countries on six continents, including at least one in New York.

17. In all, the 8,779 emails that Respondents sent to Hotmail's spam traps contained more than 40,000 instances of fraudulent and deceptive conduct. The following paragraphs describe in detail Respondents' deceptive acts and practices, and are supported by illustrative exhibits and a chart which segregates the fraudulent and deceptive conduct by ad campaign and type of conduct.

See Exh. 23 (Chart Detailing Respondents' Fraudulent Emails). Because the public disclosure of the emails would expose email addresses of spam traps used as part of efforts to protect consumers from this type of fraudulent and deceptive spam, only illustrative emails have been included as exhibits.

EMAIL: BODY AND HEADERS

18. Any email has two fundamental parts: the headers and the body. The headers are the code behind the simple "To:," "From:," and "Subject:" lines that most email users see, and are the lines of text at the beginning of an email code that document the path from the sender to the recipient. In the example below, the first 21 lines are the headers:

X-Receiver: peter_stubbs50
X-HmXmrAuthLevel: J
X-Message-Info: H83ySVbTRY3FWeNr9Ikeu7Nxksohs9II
→ **Received: from mailin-04.mx.aol.com ([219.237.125.26]) by mc3-f26.law16.hotmail.com with Microsoft SMTPSVC(5.0.2195.5600);**
Sun, 18 May 2003 20:20:47 -0700
→ **Subject: fwd: peter_stubbs50**
→ **From: "aol.com" <peter_stubbs50@aol.com>**
Content-Transfer-Encoding: 8bit
Received: from mailin-04.mx.aol.com by 2ar26.mailin-04.mx.aol.com with SMTP for peter_stubbs50@hotmail.com; Sun, 18 May 2003 23:20:37 -0600
Date: Sun, 18 May 2003 23:20:37 -0600
→ **To: peter_stubbs50@hotmail.com**
X-MSMail-Priority: Normal
X-Priority: 3
Message-Id: <98bylq4b8j6g$9fhm8x7tu9.peter_stubbs50@aol.com>
X-Mailer: MIME-tools 5.503 (Entity 5.501)
Content-Type: text/html; charset="iso-8859-1"
Importance: Normal
Return-Path: peter_stubbs50@aol.com
X-OriginalArrivalTime: 19 May 2003 03:20:48.0676 (UTC) FILETIME=[A4BECE40:01C31DB5]
<TABLE WIDTH=550 BORDER=0 align="center" CELLPADDING=0 CELLSPACING=0><TR><TD COLSPAN=3>
→ ****
<IMG SRC="http://img1.offerstream.com/ggw/ggw1_01.gif" ALT="" WIDTH=550 HEIGHT=146 border="0"></TD>
</TR><TR><TD COLSPAN=3><IMG SRC="http://img1.offerstream.com/ggw/ggw1_02.jpg" WIDTH=550 HEIGHT=306 ALT=""></TD>
</TR><TR><TD><IMG SRC="http://img1.offerstream.com/ggw/ggw1_03.jpg" WIDTH=161 HEIGHT=91 ALT=""></TD>
<TD><IMG SRC="http://img1.offerstream.com/ggw/ggw1_04.gif" WIDTH=210 HEIGHT=91 ALT=""></TD>
<TD><IMG SRC="http://img1.offerstream.com/ggw/ggw1_05.jpg" WIDTH=179 HEIGHT=91 ALT=""></TD>
</TR><TR><TD COLSPAN=3> <a
href="http://creative.offerstream.com/sc.php?addcode=CD32&bannerid=603&optionalinfo=wsb">

<IMG SRC="http://img1.offerstream.com/ggw/ggw1_06.gif" ALT="" WIDTH=550 HEIGHT=69 border="0"></TD>
</TR></TABLE>

See Exh. 24 (Respondents' May 13, 2003 email to "Peter_Stubbs50@hotmail.com" re: BannerId=639). Although headers contain a wealth of information about the email's history, they can also be deceptive because they can be easily forged. The fraudulent and deceptive conduct that Respondents engaged in, detailed below, relates to three lines in the headers: the "Received:" line, the "Subject:" line, and the "From:" line (the first three lines of **bold** text above). The other important line in the header is the "To:" line, which identifies the recipient (the fourth line in **bold** text above).

19. The body of an email is the portion below the headers and contains the content of the message. That message may appear as an image or as text. In the example in ¶ 18, above, the body of Respondents' emails contains codes inserted by Synergy6 and OptInRealBig that track their affiliates and the applicable ad campaign. *See* Exh. 1 (Ip Aff. at ¶¶ 9, 13-15, 18-20, 29) Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 21 (Synergy6 Documents Re: Delta Seven Registrations and Payments to OptInRealBig). In the example above (¶ 18), for instance, the following line of code was embedded by Respondents in their emails promising two "Girls Gone Wild" DVDs to consumers who agree to receive even more email from Synergy6:

<a href="http://creative.offerstream.com/sc.php?addcode=CD32&bannerid=603&optionalinfo=wsb">

The domain "offerstream.com" indicates that the message is from Offerstream, Synergy6's affiliate marketing program. The code "CD32" is the affiliate code Synergy6 uses to designate OptInRealBig and Richter as an affiliate. *See* Exh. 1 (Ip Aff. at ¶ 9); Exh. 13 (Synergy6 Documents Re: "CD32" and Offerstream Terms and Conditions). The code "bannerid=603" is

the code that Synergy6 uses to designate the ad campaign for its co-registration web site offer of two "Girls Gone Wild" DVDs. *See* Exh. 1 (Ip Aff. at ¶ 22); Exh. 35 (Synergy6 Ad Copy for BannerId=603). Finally, the "optionalinfo=wsb" is the code that OptInRealBig used to designate Respondents Delta Seven, Boes, and Cole as the affiliates who actually sent the email. *See* Exh. 1 (Ip Aff. at ¶¶ 14, 15, 18-20); Exh. 18, (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 21 (Synergy6 Documents Re: Delta Seven Registrations and Payments to OptInRealBig). This information permits Synergy6 and OptInRealBig to track how many consumers register at Synergy6's web sites, and which affiliate sent the email to those consumers. *See* Exh. 21 (Synergy6 Documents Re: Delta Seven Registrations and Payments to OptInRealBig).

RESPONDENTS USED FALSE IDENTITIES, FALSE EMAIL ADDRESSES, DECEPTIVE SUBJECT LINES, AND FALSE SOURCE INFORMATION IN ORDER TO HIDE WHO WAS SENDING THEIR EMAILS

20. Between May 13, 2003 and June 13, 2003, Respondents sent 8,779 emails to Hotmail spam traps. These emails promoted seven different ad campaigns each trying to entice consumers to register at a Synergy6 co-registration web site with the promise of free product samples (bannerid=62), free earrings (bannerid=389), free sunglasses (bannerid=585), free CD-Rs (bannerid=587), free "Girls Gone Wild" DVDs (bannerid=603), free donuts (bannerid=639), or a free toothbrush (bannerid=706). *See* Exh. 1 (Ip Aff. at ¶ 21, 22); Exh. 24-30 (Respondents' Emails to "Peter_Stubbs50@hotmail.com"); Exh. 31-37 (Synergy6 Ad Copy for Each Ad Campaign). Each email contained code revealing Respondents as the source. These emails were fraudulent and deceptive, as described below.

A. False Sender Identities

21. The sender identity of an email is one of the first pieces of information consumers see when their email in-box is opened. The sender identity is the name listed under the "From:" column in a typical email in-box. When the email is opened, the sender identity is the name immediately following the word "From:". In the example supra at ¶ 18, for instance, the sender purports to be "aol.com." *See* Exh. 27.

22. Of the 8,779 emails Respondents sent to the Hotmail spam traps, 7,599 emails falsely identified the sender, employing 2,990 different sender identities.

- 5,153 of these emails falsely identified the sender as the recipient's user name (with underscores and numbers removed);
- 1,515 of these emails falsely identified the sender by employing the user name from the corresponding false email address at any one of 100 domains, none of which is registered to Respondents. *See, e.g.*, Exh. 30 (sender identity is "Anneliese" and sender's email address is "Anneliese@OneShoppingCart.org").
- 269 of these emails falsely identified the sender as "Confirmations"; and
- As in the example supra at ¶ 18, 662 of these emails falsely identified the sender as one of the following eight other companies: AOL, Bigfoot, Lycos, United Online, Earthlink, Yahoo, Hotmail, and Input Output Marketing, Inc.).

See Exh. 23 (Chart Detailing Respondents' Fraudulent Emails).

B. False Sender Email Addresses

23. In addition to the sender's identity, the sender's email address is another material identifier. The sender's email address follows the sender identity in the "From:" line. Thus, in

the example supra at ¶ 18, the sender's email address purports to be "peter_stubbs50@aol.com." *See* Exh. 27.

24. Of the 8,779 emails Respondents sent to Hotmail spam traps, every single one of them falsely identified the sender's email address as any one of 7,030 different email addresses. Furthermore:

- 7,264 of these 8,779 emails falsely identified the sender's email address as one having the same user name as the recipient, at one of the following eight domains: Bigfoot.com, AOL.com, Yahoo.com, Earthlink.net, Lycos.com, Untd.com, Stormnetwork.us, or Hotmail.com.
- 1,515 of these 8,779 emails falsely identified the sender's email address as a random user name at any one of 100 domains, none of which is registered to Respondents. *See, e.g.*, Exh. 30 (sender's email address is "Anneliese@OneShoppingCart.org").

See Exh. 23 (Chart Detailing Respondents' Fraudulent Emails). Of the 8,779 emails purportedly sent from 7,030 different addresses, 808 falsely indicate that they were sent from the same Hotmail spam trap email accounts. *See, e.g.*, Exh. 1 (Ip Aff. at ¶ 23); Exh. 38 (Respondents' Emails Routed Through Server at IP Address 66.9.76.25) (emails purportedly sent from Hotmail spam trap email accounts: "flird@hotmail.com," "arkfall@hotmail.com," "kassa17@hotmail.com," "gooseil@hotmail.com," "craca@hotmail.com," "bobhave@hotmail.com," "bzliteyr9@hotmail.com," "arkinfo@hotmail.com," "smkoenen@hotmail.com," "jake665@hotmail.com"). And at least one consumer complained to Synergy6 and Richter that Respondents' email to his Hotmail account falsely appeared to be sent

from his own Earthlink.net email account. *See* Exh. 1 (Ip Aff. at ¶ 24); Exh. 39 (Consumer Complaint re: Respondents' Abuse of Consumer's Email Address).

C. False Email Server Names

25. Another means of identifying any email's source is by identifying the email server that originally sent the email. In the example supra at ¶ 18, the email server from which Respondents purportedly sent the email is: **mailin-04.mx.aol.com**. *See* Exh. 27. It is contained in the "Received:" line.

26. An email server is analogous to a mail sorting machine at the post office: it is simply a computer designed to read a recipient's email address, and then forward the email along the path toward the recipient. An email generally travels through a number of servers on its path from the sender to the recipient. These email servers each stamp the email with the server's name and identifying information so as to create a record of the path of its travels, akin to a customs agent stamping a visitor's passport to document his or her travels. A typical email will have several "Received:" lines identifying the servers that have handled the email along its path.

27. There exist, however, insecure servers, like insecure borders, where those wanting to hide their travels can pass. Because these servers are not email servers, they cannot record any information to be inserted into the email headers. Thus, when an email is routed through these insecure servers, the only information in an email's headers regarding the email server that sent the email is that which the sender explicitly provides. In all 8,779 emails sent to the Hotmail spam traps, Respondents caused the email server from which the email originated to be falsely identified as any one of 123 different email servers at 108 different domains. Moreover:

- In 7,264 of these 8,779 emails, the Respondents caused the email server from

which the email originated to be falsely identified as any one of 23 servers at eight different domains: Bigfoot.com, AOL.com, Yahoo.com, Earthlink.net, Lycos.com, Untd.com, Stormnetwork.us, or Hotmail.com.

- In 1,515 of these 8,779 emails, the Respondents caused the email server from which the email originated to be falsely identified as any one of 100 servers at 100 different domains.

See Exh. 23 (Chart Detailing Respondents' Fraudulent Emails). In each of the 8,779 emails, the email falsely purports to originate at a mail server that is at the same domain as the falsified sender's email address.

D. False Originating Internet Protocol Addresses

28. Like all properly configured email servers, the Hotmail email servers stamped the headers of the deceptive emails with the Internet Protocol Address of the server from which they received the emails. An Internet Protocol Address ("IP address") is the numerical code that identifies computers on a network. It is a set of four numbers, each one ranging from 0 to 255, separated by periods. IP addresses are used to direct Internet traffic to and from specific computers.

29. In the example supra at ¶ 18, for instance, the IP address of the server that forwarded Respondents' email to the Hotmail spam trap is identified in the "Received:" line, following the falsified email server name, as: **219.237.125.26**. *See* Exh. 27. This IP address is not assigned to any of the Respondents, but rather is assigned to a company in China called Beijing Gehua CATV Network Co., Ltd. *See* Exh. 1 (Ip Aff. at ¶ 25); Exh. 43 (IP Address 219.237.125.26 Registration Page). In fact, Respondents have a vast pattern of deceptively identifying the IP address from which their emails originate: each of the 8,779 emails caught in the spam traps

were from any of 514 different servers, in 35 countries, on six continents. *See* Exh. 41 (Chart of IP Addresses of Servers Through Which Respondents Routed Emails). None of these IP addresses was actually registered to Respondents. *See id.*

30. One such server that was falsely identified in this way is located in New York City. Of the 8,779 emails caught in the Hotmail spam traps, 77 came from a server with the assigned IP address 66.9.76.25. *See* Exh. 38 (Respondents' Emails Routed Through Server at IP Address 66.9.76.25). This IP address is assigned to a New York City based Internet Service Provider, IntelliSpace, which had leased it to its corporate client, New York City based Warjo Promotions, Inc. *See* Exh. 1 (Ip Aff. at ¶ 26); Exh. 42 (Affidavit of Joe Carey); Exh. 44 (IP Address 66.9.76.25 Registration Page). Warjo is a promotional products company that does not send bulk commercial email, nor has it given permission or authority to anyone else to use its servers to send commercial email from its servers. *See* Exh. 42 (Affidavit of Joe Carey).

31. After Respondents sent their emails to the Hotmail spam traps from Warjo's server, consumers complained to IntelliSpace mistakenly believing that one of its clients was sending fraudulent spam or allowing others to do so. *See* Exh. 1 (Ip Aff. at ¶ 27); Exh. 45 (Consumer Complaints to IntelliSpace re: Open Proxy Server at 66.9.76.25).

E. False and Deceptive Subject Lines

32. In addition to falsely identifying the source of their emails, Respondents included false and deceptive subject lines in their emails, in an attempt to trick consumers into opening emails they otherwise would not. In the example supra at ¶18, for instance, the subject line is: **"Subject: Fwd: peter_stubbs50"**, which falsely indicates that the email is being passed along from another person. *See* Exh. 27. In many of the 8,779 emails, Respondents included false or

deceptive subject lines:

- 3,596 of Respondents' emails falsely indicated that the email was a response to previous email by starting the subject line with the abbreviation "Re:," the standard indicator signifying that an email is a response to an email from the recipient, rather than unsolicited;
- 2,830 of Respondents' emails falsely indicated that the email was being passed along from another sender, by starting the subject line with the abbreviation "Fwd:," the standard indicator signifying that an email has been forwarded from a previous recipient, rather than sent by its original author; and
- 1,039 of Respondents' emails falsely indicated they were sent from or on behalf of one of eight of the following companies: AOL, Bigfoot, Lycos, United Online, Earthlink, Yahoo, Hotmail, and Input Output Marketing, Inc.

See Exh. 23 (Chart Detailing Respondents' Fraudulent Emails).

33. These 8,779 emails contain more than 40,000 instances of deceptive conduct, forged headers, and misleading information. *See id.* Moreover, this number reflects only the number of fraudulent emails that happened to have been sent to Microsoft's spam traps, and is a minuscule fraction of the total violations committed by the Respondents.

RESPONDENTS CONTINUED TO SEND FRAUDULENT EMAIL, AND TO ACCEPT ITS COMMERCIAL BENEFITS AFTER RECEIVING COMPLAINTS

34. Days after Respondents began flooding the Hotmail spam traps with their emails, consumers began sending complaints to both Synergy6 and Richter detailing the fraud, which

Synergy6 observed were "scathing." *See* Exh. 1 (Ip Aff. at ¶ 28); Exh. 12 (Synergy6 Emails Between Synergy6 Employees and OptInRealBig Employees), Exh. 46 (Complaints to Synergy6 and OptInRealBig re: Spam with Forged Headers). Richter and Champion both had firsthand knowledge of these complaints, personally discussing with each other and co-workers via email the "scathing complaints" they were receiving from consumers. *See* Exh. 12 (Synergy6 Emails Between Synergy6 Employees and OptInRealBig Employees). Richter also discussed these complaints with Boes and Cole. *See* Exh. 1 (Ip Aff. at ¶¶ 14-16). Nonetheless, Respondents continued to send the fraudulent and deceptive spam for more than a month. All defendants received material economic and commercial benefits from this scheme. *See* Exh. 1 (Ip Aff. at ¶¶ 15, 18, 19, 29); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 47 (OptInRealBig Invoices and Synergy6 Checks for May and June 2003). For instance, by the end of the month, the fraud-ridden emails generated 20,409 new leads to whom Synergy6 could (and presumably did) market. *See* Exh. 21 (Synergy6 Documents Re: Delta Seven Registrations and Payments to OptInRealBig). Synergy6 paid a commission for each lead generated to OptInRealBig, who, in turn, paid Boes and Cole through Delta Seven. *See* Exh. 1 (Ip Aff. at ¶¶ 15, 18, 19, 29); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 47 (OptInRealBig Invoices and Synergy6 Checks for May and June 2003).

THE INDIVIDUAL DEFENDANTS ARE PERSONALLY LIABLE

35. Both Richter and Champion excercised control of their respective companies' material day-to-day corporate operations. Champion handled many aspects of his company's operations, including negotiating commissions, making arrangements to pay affiliates, and determining how

much email affiliates should send. *See* Exh. 12 (Synergy6 Emails Between Synergy6 Employees and OptInRealBig Employees). Richter, likewise, handled technical problems, negotiated list acquisitions, sought payments from debtors, sent ad copy to affiliates, and responded to complaints from consumers and ISPs. *See* Exh. 12 (Synergy6 Emails Between Synergy6 Employees and OptInRealBig Employees); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests). Boes and Cole personally sent the fraudulent emails, and were paid for their efforts. *See* Exh. 1 (Ip Aff. at ¶¶14-16, 18-20); Exh. 18 (Email Correspondence Between OptInRealBig and Delta Seven and Corresponding Wire Transfer Requests); Exh. 21 (Synergy6 Documents Re: Delta Seven Registrations and Payments to OptInRealBig). As discussed supra, Richter and Champion had personal knowledge of the fraudulent emails sent by Boes and Cole within days of their delivery.

LARGE AMOUNTS OF FRAUDULENT
SPAM WAS SENT TO RESIDENTS OF NEW YORK

36. On information and belief, Respondents have sent millions of their deceptive and unlawful emails to consumers. On information and belief, approximately five percent of these consumer recipients were New York residents. An accounting of the total emails sent, as well as the percentage of Synergy6's registrants who are New York residents, as sought in the Verified Petition, would reveal an estimated total of emails containing violations. At a minimum, the Petitioners seek penalties in the amount of $500 per violation, based on the number of registrants from Respondents' deceptive and unlawful emails who are New York residents.

NOTICE OF ACTION AND
OPPORTUNITY TO RESPOND AND BE HEARD

37. Prelitigation notice as provided for in N.Y. GBL § 349 and § 350-c has been given, by

certified mail delivered on five or more days notice to Respondents. *See* Exh. 48 (Certified Letters to Respondents Containing Notice of Proposed Litigation).

CONCLUSION

38. Respondents repeatedly and persistently have engaged in fraudulent, deceptive, and illegal acts in the course of conducting their email marketing businesses. They are responsible for sending untold amounts of spam containing false headers and routing information and deceptive subject lines. They have hidden behind thousands of fake identities and email addresses, and utilized hundreds of servers worldwide that were not their own, in order to prevent consumers from identifying them as the source of unwanted junk mail.

39. Accordingly, Petitioners respectfully request that the court enjoin Respondents from using false or misleading information in the headers of commercial emails; enjoin Respondents from causing the original source of their commercial emails to be falsely identified; enjoin Respondents from using false or misleading subject lines in their commercial emails; require Respondents to disgorge any profits derived from their illegal activities; require each Respondent, prior to continuing any business activities in or directed to New York, to post a bond in the amount of $100,000 to protect future consumers; and to award costs and penalties as authorized by statute, and such other relief as requested herein.

WHEREFORE, the Attorney General respectfully requests that the Court grant the relief sought in the accompanying Verified Petition.

Dated: December 17, 2003
New York, New York

Stephen Kline
Assistant Attorney General
Internet Bureau
Attorney for Petitioner
120 Broadway, 3rd Floor
New York, New York 10271
(212) 416-8433