

**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-

**MONSTERHUT, INC.
d/b/a MONSTERHUT.COM, and
Todd Pelow and Gary Hartl, individually,**

Respondents.

Index No. 402140/2002

LOTTIE WILKINS, J.S.C.

**MEMORANDUM IN SUPPORT
OF VERIFIED PETITION OF ATTORNEY GENERAL**

ELIOT SPITZER
Attorney General of the State of New York,
Attorney for Petitioner
Internet Bureau
120 Broadway, 3rd Floor
New York, NY 10271
Tel: (212) 416-6250
Fax: (212) 416-8369

KENNETH DREIFACH
Assistant Attorney General in Charge

Stephen Kline
Assistant Attorney General
of counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....i

PRELIMINARY STATEMENT.....1

STATEMENT OF FACTS.....2

 1.Respondents.....3

 2.The Internet, Email, and Spam: Background.....4

 3.The Widely Accepted Distinction Between Opt-in vs.
 Opt-out Email Lists.....6

 4.Monsterhut’s Deceptive Spamming, and the Fourth Department’s Holding.....8

 5.MonsterHut Has Effectively Admitted That it is *NOT* an “Opt-in” Emailer.....9

ARGUMENT.....13

RESPONDENTS REPEATEDLY HAVE
VIOLATED GBL §§ 349 AND 350, EACH OF
WHICH IS ACTIONABLE UNDER EXECUTIVE LAW § 63(12).....13

 A.Respondents’ Conduct Violates GBL § 349.....14

 B.Respondents’ Conduct Also Violates GBL § 350.....16

 C. Respondent has Asserted No Valid or Even Cognizable Defenses.....18

BECAUSE RESPONDENTS HAVE RAISED
NO TRIABLE ISSUE OF FACT, THE PETITION
MUST BE GRANTED AND NO HEARING IS REQUIRED.....20

THE ATTORNEY GENERAL IS ENTITLED TO
INJUNCTIVE RELIEF, A PERFORMANCE BOND, PENALTIES AND COSTS.....22

THE INDIVIDUAL RESPONDENTS ARE
PERSONALLY LIABLE FOR THE REPEATED
AND PERSISTENT FRAUDULENT, DECEPTIVE AND
ILLEGAL ACTS ALLEGED IN THE PETITION.....25

CONCLUSION.....29

TABLE OF AUTHORITIES

Cases

<u>America Online, Inc. v. IMS et al</u> , 24 F. Supp. 2d 548 (E.D. Va. 1998)	6 n. 4
<u>America Online, Inc. v. Nat. Health Care Discount, Inc.</u> 121 F. Supp.2d 1255 (N.D. Iowa 2000)	6
<u>BeaverHome.com et al v. Mail Abuse Prevention System et al.</u> (01 cv 0598) (W.D. N.Y. 2001)	8, 11
<u>Benrus Watch Co. v. F.T.C.</u> , 352 F.2d 313, 325 (8th Cir. 1965), <u>cert. denied</u> , 384 U.S. 939 (1966)	26
<u>CompuServe, Inc. v. Cyber Promotions</u> , 962 F. Supp. 1015, 1018 (S.D. Ohio 1997)	6 n.4
<u>Consumer Sales Corp. v. F.T.C.</u> , 198 F.2d 404 (2d Cir.), <u>cert. denied</u> , 344 U.S. 912 (1952)	26
<u>F.T.C. v. Amy Travel Service, Inc.</u> , 875 F.2d 564 (7th Cir. 1989)	26
<u>Ferguson v. FriendFinders, Inc.</u> , 94 Cal. App. 4 th 1255 (Cal. App. 1 st Dist. 2002)	5
<u>Geismer v. Abraham & Strauss</u> , 109 Misc.2d 495 (Sup. Ct. Suffolk Co. 1981)	17, 19 n.10
<u>In re McGrath</u> , 7 B.R. 496 (S.D.N.Y. 1980)	25
<u>Lefkowitz v. Bull Investment Group, Inc.</u> , 46 A.D.2d 25 (3d Dep't. 1974), <u>appeal denied</u> , 35 N.Y.2d 647 (1975)	13, 14, 19 n.10
<u>Lefkowitz v. E.F.G. Baby Products</u> , 40 A.D.2d 364 (3d Dep't 1973)	14, 19 n.10
<u>Lefkowitz v. McMillen</u> , 57 A.D.2d 979 (3d Dept.), <u>motion for leave to appeal denied</u> , 42 N.Y.2d 807 (1977)	21, 22

<u>Lefkowitz v. Therapeutic Hypnosis,</u> 83 Misc.2d 1068 (Sup. Ct. Alb. Co. 1975), <u>rev'd on other grounds, 52 A.D.2d 1017 (3d Dept. 1976)</u>	24
<u>Lippman Packing Corp. v. Rose,</u> 203 Misc. 1041 (N.Y. Mun. Ct. 1953)	25
<u>Marine Midland Bank v. John C. Russo Produce,</u> 50 N.Y.2d 31 (1980)	25
<u>Media3 Techs., LLC v. Mail Abuse Prevention Sys.,</u> 2001 U.S. Dist. LEXIS 1310 (D. Mass. Jan. 2, 2001)	1 n.1, 6
<u>Meyers Bros. Parking Sys. v. Sherman,</u> 87 A.D.2d 562, 563 (1st Dept.), <u>aff'd</u> , 57 N.Y.2d 653 (1982)	24
<u>MonsterHut v PaeTec,</u> 107189 cv 2001 (Sup. Ct. Niagara Co. 2001)	4
<u>MonsterHut, Inc. v. PaeTec Comm., Inc.,</u> 741 N.Y.S.2d 820 (4 th Dep't 2002)	1-2, 3, 8
<u>People v. 21st Century Leisure Spa International, Ltd.,</u> 153 Misc.2d 938 (Sup. Ct. N.Y. Co. 1991)	26-27
<u>People v. Allied Marketing Group, Inc.,</u> 220 A.D.2d 370 (1 st Dep't. 1995)	14, 21, 25
<u>People v. Anderson,</u> 137 A.D.2d 259 (4 th Dep't 1988)	14
<u>People v. B.C. Associates, Inc.,</u> 22 Misc.2d 43 (N.Y. Co. 1959)	20
<u>People v. Compact Associates,</u> 22 A.D.2d 129 (1st Dept. 1964)	23
<u>People v. Concert Connection, Ltd.,</u> 211 A.D.2d 310 (2 nd Dep't 1995)	25
<u>People v. Court Reporting Institute,</u> 245 A.D.2d 564 (2d Dep't 1997)	26

<u>People v. Empyre Inground Pools, Inc.,</u> 227 A.D.2d 731 (3d Dep't 1996)	14 n.5, 25, 26
<u>People v. Federated Radio Corp.,</u> 244 N.Y. 33 (1926)	13
<u>People v. Helena VIP Personal Introduction Service of New York, Inc.,</u> 199 A.D.2d 186 (1 st Dept. 1993)	21, 22, 25
<u>People v. Volkswagen of America, Inc.,</u> 47 A.D.2d 868 (1st Dept. 1975)	17
<u>State of New York v. Apple Health and Sports Clubs, Ltd., Inc.,</u> 80 N.Y.2d 803 (1992)	25, 26
<u>State of New York v. British & American Casualty Co.,</u> 133 Misc. 2d 352 (Sup. Ct. N.Y. Co. 1986)	14 n.5
<u>State of New York v. Colorado State Christian College,</u> 76 Misc.2d 50 (Sup. Ct. N.Y. Co. 1973)	15, 17, 19 n.10
<u>State of New York v. Daro Chartours,</u> 72 A.D.2d 872 (3d Dept. 1979)	20, 21-22, 23, 24
<u>State of New York v. Lipsitz,</u> 174 Misc. 2d 571 (Sup. Ct. N.Y. Co. 1997)	14, 15, 16 n.7, 18
<u>State of New York v. Management Transition Resources, Inc.,</u> 115 Misc. 2d 489 (Sup. Ct. N.Y. Co. 1982)	15, 21
<u>State of New York v. Person,</u> 75 Misc.2d 252 (Sup. Ct. N.Y. Co. 1973)	23
<u>State of New York v. Princess Prestige,</u> 42 N.Y.2d 104 (1977)	14, 23
<u>State of New York v. Scottish-American Ass'n,</u> 52 A.D.2d 528 (1 st Dep't), <u>appeal dismissed</u> , 39 N.Y.2d 1057 (1976)	14, 21 n.11, 23
<u>State v. Abandoned Funds Information Ctr., Inc.,</u> 129 Misc.2d 614 (Sup. Ct. N.Y. Co. 1985)	17
<u>State v. Midland Equities of New York,</u> 117 Misc.2d 203 (Sup. Ct. N.Y. Co. 1982)	21, 23, 24

<u>State v. Waterfine Water Conditioning Co. of New York, Inc.</u> , 87 Misc.2d 18 (Sup. Ct. Albany Co. 1975)	21
<u>United States v. Readers Digest Association, Inc.</u> , 662 F.2d 955 (3d Cir. 1981)	24
<u>Verizon Online Serv., Inc. v. Ralsky</u> , 203 F. Supp. 2d 601 (E.D. Va. 2002)	6 n.4

Other Authorities

CPLR § 3212	21
CPLR § 409(b)	21
CPLR § 8303(a)(6)	24
David Sorkin, <u>Technical and Legal Approaches to Unsolicited Electronic Mail</u> , 35 U.S.F. L. Rev. 325 (2000)	5
Executive Law § 63(12)	<i>passim</i>
Fay Jones, <u>Spam: Unsolicited Commercial E-Mail by Any Other Name</u> , 14 J. Internet L. (Sept. 1999)	6
N.Y. General Business Law § 349 (McKinney's)	<i>passim</i>
General Business Law § 350 (McKinney's)	<i>passim</i>
National Telecomm. and Information Admin. U.S. Dep't of Commerce, <u>A Nation Online: How Americans Are Expanding Their Use of the Internet</u> , (2002)	4
Scot Graydon, <u>Much Ado About Spam: Unsolicited Advertising, the Internet, and You</u> , St. Mary's L.J. 77 (2000)	5
Siegel, <u>New York Practice</u> § 547 (2d ed. 1991)	20
The Fraud Bureau, <u>The Cost of Spam</u> (1999) (visited July 31, 2002)	6 n.3

Petitioners, the People of the State of New York, by Eliot Spitzer, Attorney General of the State of New York, submit this Memorandum of Law in support of their Petition for injunctive relief, posting of a performance bond, penalties and costs pursuant to Executive Law § 63(12) and General Business Law §§ 349 and 350.

PRELIMINARY STATEMENT

Unsolicited email, widely known as “spam,” is a monumental source of annoyance for modern consumers. Worse than this annoyance, it adds considerable costs to internet service systems, because it is the system providers (“Internet service providers” or “ISPs”) and consumers who access their emails – not the senders – who must pay most of the cost of its delivery. In the words of one court, “[r]eceiving spam is like receiving . . . a collect call from a telemarketer or junk mail on which you have to pay the postage.”¹

The senders of spam – spammers – are therefore widely disliked in the Internet community. They are denied access to Internet systems, and their mail is ignored *en masse* by recipients. Yet because the cost to senders of delivering this Internet “junk mail” is so minimal, the spam keeps coming.

Standing in contrast to these spammers are more sophisticated “permission-based” or “opt-in” emailers. These email marketers compile, purchase and aggregate lists of consumers who have “opted in” to, or requested placement on, certain email lists.

Respondent Monsterhut is without question a spammer – in fact, the Fourth Department has so held, as a matter of law. See *Monsterhut, Inc. v. PaeTec Comm., Inc.*, 741 N.Y.S.2d 820

¹ Media3 Techs., LLC v. Mail Abuse Prevention Sys., 2001 U.S. Dist. LEXIS 1310, at *3 fn. 1 (D. Mass. Jan. 2, 2001).

(4th Dep't 2002) (holding that Monsterhut violated its agreement with an ISP by sending "unsolicited, mass, commercial email in breach of the agreement"). But, contrary to New York consumer protection laws, Monsterhut repeatedly has lied about this fact – to consumers, ISPs, and even its own advertising clients, in order to boost its credibility and therefore its profits. Namely, in multiple emails and communications with these entities, Monsterhut has falsely held itself out as a "permission based" or "opt-in" email marketer. In fact, Monsterhut has represented that its emails are "100 % permission based."

Monsterhut's misrepresentations about the very nature of its business and its services constitute deceptive practices, false advertising, and fraudulent and illegal practices, under New York GBL § 349-350 and Executive Law § 63(12). Having sought to prosper -- and indeed prospered until it was caught -- from its demonstrably false statements, Monsterhut has engaged in deceptive practices and fraudulent and illegal conduct. Only a clear holding from this Court establishing that such acts are deceptive and fraudulent will protect consumers and system operators alike from Monsterhut and, hopefully, other equally notorious phony emailers.

We therefore ask that this Court grant the Petition in full, enjoin the deceptive behavior set forth herein, award the state costs and penalties, and require respondents to post a performance bond to protect consumers and ISPs alike from future illegal acts, and to deter respondents from engaging in similar practices in the future.

STATEMENT OF FACTS

As set forth fully in the Verified Petition ("Petition") and in the Affirmation of Assistant Attorney General Stephen Kline, dated May 17, 2002 ("Kline Aff."), this special proceeding is brought by the Attorney General to enjoin the fraudulent, deceptive and unlawful practices of

respondents and to seek costs and penalties and a performance bond. Specifically, the Petition alleges that in an attempt to induce consumers to respond to their commercial email solicitations, respondents deceptively told consumers that they had requested the solicitations.

1. Respondents

A. MonsterHut, Inc.

MonsterHut, Inc. ("MonsterHut") is a corporation organized under the laws of Delaware, with its principal place of business in Niagara Falls, New York. Although MonsterHut maintains its corporate office in the State of New York and all of MonsterHut's operations take place from the State of New York, it has never filed a Certificate of Incorporation with the Secretary of State. MonsterHut promotes itself as a legitimate permission-based online marketing company with a website (<http://www.monsterhut.com>) that promotes its work, displays its privacy policy, and contains a page where consumers who have received commercial email from MonsterHut can request to be removed from its database.

MonsterHut has sent consumers more than one-half billion commercial emails since March 2001. Squarely contrary to numerous false statements by MonsterHut more fully described herein, many of their emails are unsolicited. Therefore, the Appellate Division, Fourth Department has accurately described MonsterHut's email marketing as "spamming." MonsterHut, Inc. v. PaeTec Comm., Inc., 741 N.Y.S.2d 820, 821 (4th Dep't 2002) (thus holding that Monsterhut had violated its agreement with an ISP, by sending "unsolicited, mass, commercial email in breach of the agreement").

B. Todd Pelow

Todd Pelow is the Chief Executive Officer of MonsterHut, Inc. Pelow has been actively

involved in the daily operations of MonsterHut. His broad duties have ranged from negotiating contracts with ISPs to handling customer and consumer complaints; he is knowledgeable as to how MonsterHut generates and obtains lists of email addresses which it uses in its commercial email campaigns. See Kline Aff. Exhs. 8-13 (attaching Affidavits of Todd Pelow respectively dated Jan. 4, 2002, March 21, 2001, May 11, 2001, Dec. 7, 2001, March 28, 2001, and Jan. 22, 2002, each filed in MonsterHut, Inc. v. PaeTec Comm., Inc., 107189 cv 2001 (Sup. Ct. Niagara Cty.) (hereinafter "PaeTec Litigation")).² In response to the Petition, Pelow has filed an affidavit on behalf of himself and the corporation.

C. Gary Hartl

Gary Hartl is the Chief Technology Officer of MonsterHut, Inc. and has overseen all of the targeted email sent out by MonsterHut.com since March 15, 2001. He is knowledgeable as to how MonsterHut generates and obtains lists of email addresses which it uses in its commercial email campaigns. See Kline Aff. Exh. 14 (Affidavit of Gary Hartl in Support of a Preliminary Injunction, dated May 11, 2001, filed in PaeTec Litigation). Though properly served, Hartl has not responded to the instant Verified Petition.

2. The Internet, Email, and Spam: Background

Currently, more than 150 million Americans use the Internet and one half of all Americans use email. See National Telecomm. and Information Admin. U.S. Dep't of Commerce, A Nation Online: How Americans Are Expanding Their Use of the Internet, pp. 1, 2, 29 (2002). While email is thus extremely popular, "spam," or unsolicited bulk email, is widely

² As used herein, "PaeTec Litigation" refers to the proceedings in the trial court, in Monsterhut, Inc. v. PaeTec Comm., Inc., rather than the Fourth Department's opinion.

condemned by consumers, and within the Internet community. See generally, Ferguson v. FriendFinders, Inc., 94 Cal. App. 4th 1255, 1268 (Cal. App. 1st Dist. 2002) (thus finding that California had a “substantial legitimate interest in protecting its citizens from the harmful effects of deceptive UCE [unsolicited commercial email]”).

Indeed, while more than half of all consumers feel positively about permission based, or “opt-in” email, i.e., email sent from lists on which they requested placement, more than eighty percent feel negatively toward unsolicited commercial email. See Kline Aff. ¶ 27 and attachments. This intense dislike of unsolicited commercial email stems from the fact that consumers resent the time it takes to process the mail, view it as an invasion of privacy, and find it offensive. See id. and attachments.

Spam affects e-commerce far beyond consumers’ annoyance with it, and the time it takes consumers to access and discard. Particularly burdensome to ISPs and consumers alike is the unique cost-shifting nature of spam. Unlike other forms of direct marketing, such as telemarketing and postal mail, it is the receiver, not the sender of spam, who largely pays the cost. David Sorkin, Technical and Legal Approaches to Unsolicited Electronic Mail, 35 U.S.F. L. Rev. 325, 338 (2000). A spammer can send millions of emails for as little as fifty dollars. See Scot Graydon, Much Ado About Spam: Unsolicited Advertising, the Internet, and You, St. Mary’s L.J. 77, 83 (2000). But those same emails consume massive amounts of network bandwidth, memory, and storage space; require ISPs to hire additional employees to block spam and answer customer complaints; and force ISPs to lose revenue due to customer defections and

new customer acquisition costs to replace customers who have defected.³

Invariably, these costs to the system are passed to consumers through higher prices for Internet access. See generally Fay Jones, Spam: Unsolicited Commercial Email by Any Other Name, 14 J. Internet L. 2, fn. 8 (Sept. 1999). In addition to increased access prices, consumers may pay additional connection costs if they are not paying a flat rate for access or must pay for phone connections. Thus, to consumers, “[r]eceiving spam is like receiving . . . a collect call from a telemarketer or junk mail on which you have to pay the postage.” Media3 Techs., LLC v. Mail Abuse Prevention Sys., 2001 U.S. Dist. LEXIS 1310, at *3 fn. 1 (D. Mass. Jan. 2, 2001).

ISPs and consumers alike thus have expended considerable resources detecting and fighting spam. For instance, ISPs filter email, and try to block spammers from their network when they violate ISPs’ policies.⁴ But spammers counter filtering by disguising the nature or source of the spam, or by using other techniques to deceive ISPs and the public alike. See generally America Online, Inc. v. Nat’l. Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1259-60 (N.D. Iowa 2000) (detailing the ongoing technological struggle between spammers and system operators).

3. The Widely Accepted Distinction Between Opt-in vs. Opt-out Email Lists

In the field of email marketing, the terms “opt-in” and “opt-out” have clearly defined meanings, widely accepted by industry, regulators, and consumers. See Kline Aff. ¶¶ 10-17.

³ See The Fraud Bureau, The Cost of Spam (1999) (visited July 31, 2002) <http://www.fraudbureau.com/articles/consumer/article14.html>; ISPs and Spam, at 12; see, e.g., America Online, Inc. v. Nat. Health Care Discount, Inc. 121 F. Supp.2d 1255, 1262 (N.D. Iowa 2000) (AOL defining its “per recipient charge” for each email as \$0.00078, or \$780 per million emails).

⁴ See generally Verizon Online Serv., Inc. v. Ralsky, 203 F. Supp. 2d 601, 606 (E.D. Va. 2002); America Online, Inc. v. IMS et al., 24 F. Supp. 2d 548 (E.D. Va. 1998). CompuServe, Inc. v. Cyber Promotions, 962 F. Supp. 1015, 1018 (S.D. Ohio 1997).

Under an opt-in protocol, consumer email addresses are collected and used only if the consumer affirmatively has approved, or “opted into,” such collection. *Id.* at ¶¶ 14-15. Under an opt-out protocol, consumer email addresses are collected and used so long as the consumer has not specifically declined, or “opted out of” such collection. *Id.* at ¶¶ 16-17.

The very significant distinction between an opt-in and an opt-out protocol thus lies in the default rule when no affirmative steps are taken by the consumer: when this occurs, the “opt in” permits a web merchant to do nothing where a consumer has failed to speak; but the “opt out” permits the merchant to do anything with a consumer’s data, when a consumer is silent in the face of a web site’s posted threat to share consumer data. The term “opt-in” is thus synonymous with the term “permission-based,” and email collected using such a protocol is considered solicited. By contrast, email collected using an “opt-out” protocol is considered unsolicited email, or spam.

Marketers commonly employ either of these two protocols by displaying a small box on a web page with an accompanying statement such as, “I agree to allow the owner of this website and its affiliates to send commercial email to me.” In an opt-in protocol, the consumer must check this box to allow the collection or use of the email address. In an opt-out protocol, this box is pre-checked and the consumer must un-check it to prevent the collection or use of the consumer’s email address.

These standard, uncontroversial definitions are accepted by industry, regulators and consumers alike. *Kline Aff.* ¶¶ 10-17. Even MonsterHut itself has acknowledged this: in prior litigation, the company submitted the following description of own practices:

MonsterHut, Inc. is a *permission based* marketing organization. A permission based protocol is one in which consumers ‘opt-in’ or affirmatively indicate to

marketing organizations, such as [MonsterHut] and others, that they would like information on a specific item of interest.

See Kline Aff. ¶ 19 and Exh. 18 (Memorandum of Law in Support of a Temporary Restraining Order and Preliminary Injunction at 4, dated Aug. 23, 2001, filed in BeaverHome.com et al v. Mail Abuse Prevention System et al, (01 cv 0598) (W.D. N.Y. 2001) (Hereinafter “MAPS Litigation”).

Consumers likewise make an unequivocal distinction between “permission-based” and unsolicited commercial email. Permission-based email is overwhelmingly preferred by consumers, while unsolicited commercial email, or spam, is largely reviled. See Kline Aff. ¶ 27.

4. Monsterhut’s Deceptive Spamming, and the Fourth Department’s Holding

Here, Monsterhut, a notorious spammer, set out to fool ISPs, consumers, and even its own advertising clients, in order to avoid being identified as a spammer. To do this, MonsterHut deceptively presented its own unsolicited emails as, alternately, “permission-based,” “100% permission based,” or “opt-in” commercial email, i.e., email that was in fact solicited by consumers. This sham allowed MonsterHut’s access to ISP systems that normally would have been denied it. Thus, the Fourth Department has held as a matter of law -- in a case addressing an ISP’s right to terminate Monsterhut’s access -- that Monsterhut had sent “unsolicited, mass, commercial email in breach of the agreement [with its ISP].” Monsterhut, 741 N.Y.S. 2d at 821. The Fourth Department likewise held that the defendant ISP had “further established as a matter of law that plaintiff had breached the agreement by engaging in spamming.” Id.

The Fourth Department’s conclusion as a matter of law that Monsterhut is a spammer also establishes as a matter of law the falsity of Monsterhut’s repeated statements (fully set forth herein) that its emails were “permission based” or “opt-in.” In truth, as Monsterhut has now

acknowledged under oath and in court papers, millions of its commercial emails are not permission based, and were sent to consumers who neither requested nor permitted such solicitations. See, e.g., Kline Aff. ¶¶ 24-25.

More specifically, MonsterHut falsely represented to consumers that every consumer who received its commercial email had opted in to receive it, whether through MonsterHut or one of Monsterhut's affiliates. Since January 2001, for instance, MonsterHut has falsely described its consumer email address lists as "permission based," "100% percent permission based," and "permission based . . . to the best of our knowledge." Kline Aff. ¶ 18. Likewise, MonsterHut's commercial emails to consumers falsely state that its lists were "opt-in" lists. Kline Aff. ¶ 20. Additionally, in response to consumer emails questioning whether its commercial email was truly unsolicited, MonsterHut has falsely replied that "[t]here is no question that your email address has been opted in" Kline Aff. ¶ 21.

In effect, Monsterhut repeatedly advertised to consumers, ISPs, and its advertising clients, that it was not a spammer, but rather an "opt-in" or "permission-based" marketer. But this was untrue. Indeed, MonsterHut does not and cannot claim it to be true, given that the Fourth Department has now held, as a matter of law, that it was a spammer.

MonsterHut's attempt to deceive consumers into believing that its unsolicited spam was really permission-based email undermines the integrity of electronic commerce, the integrity of Internet service systems, and the role commercial email plays in informing consumers' choices, including whether to respond to, or even to download or read, the solicitation.

5. MonsterHut Has Effectively Admitted That it is NOT an "Opt-in" Emailer

As if the Fourth Department's res judicata holding were not enough proof of

Monsterhut's misdeeds, MonsterHut's own sworn statements confirm that all of its above representations were false. Namely, in unrelated litigation, MonsterHut admitted that it knowingly used email lists containing addresses collected using both opt-in and opt-out protocols. Gary Hartl, who oversaw all of the commercial email sent out by MonsterHut since March 2001, explicitly confirmed that Monsterhut uses three different types of lists:

- a. Internally generated lists of individuals whom [sic] directly subscribed or requested information from MonsterHut.com's web sites.
- b. Externally generated lists of individuals who directly subscribed or requested information from affiliate partners of MonsterHut.com. *These affiliate partners have received permission or have made it explicitly known to such individuals that their email addresses will be shared with third parties.*
- c. Externally generated commercial marketing lists/databases of individuals and email addresses which were purchased by MonsterHut.com with the preconception that all the individuals included in such lists/databases were interested in receiving third party targeted email advertising (emphasis added)

Kline Aff. ¶ 24 and Exh. 14 (Affidavit of Gary Hartl in Support of MonsterHut's Motion for a Preliminary Injunction in PaeTec Litigation, at ¶¶ 7, 10, dated May 11, 2001).

Hartl's statement that MonsterHut's affiliates had either *received permission or made it explicitly known to such individuals* that their email addresses would be shared indicates that Monsterhut collected at least some email addresses under an opt-out protocol, *i.e.*, one in which consumers' permission was inferred merely from their silence. Kline Aff. ¶¶ 10-17.

In its Supporting Memo of Law in yet a different litigation, MonsterHut again admitted that -- contrary to its representations of "opt in" status -- it actually collects email addresses from consumers who have failed to take any affirmative act, but simply let a pre-checked box remain

checked:

When [consumers] opt-in to the websites of [MonsterHut.com or BeaverHome.com], or affiliates of [MonsterHut or BeaverHome] a box is *pre checked*. That *pre checked* box says, 'I would like information on other related topics'. [MonsterHut, BeaverHome], and other merchants trade barter or sell the email addresses of these willing participants in the experience known as the World Wide Web.

Kline Aff. ¶ 25 and Exh. 18 (attaching and quoting MonsterHut's Memorandum of Law in Support of a Temporary Restraining Order and Preliminary Injunction, at 4, dated Aug. 23, 2001, BeaverHome.com et al v. Mail Abuse Prevention System et al, 01 cv 0598 (W.D.N.Y 2001) (emphasis added).

In yet another memorandum -- this one in the PaeTec Litigation -- MonsterHut conceded that its affiliates really use both opt-in and opt-out protocols to collect email addresses:

It should strongly be noted that all of the individuals included in any of the lists acquired by MonsterHut have authorized said third party list developer to use and distribute their personal information in any manner that said third party list developer would see fit. . . . A brief illustration of how some of these third party list developers operate may be appropriate at this point. 'Excite' is an internet search engine which provides free email addresses to its users as one of its services. When an individual signs up for a free email address on Excite he or she must fill out an online form in which all of the individuals personal information is entered. Some of these online forms are more complex than others but a majority of them include areas in which the individual can indicate likes and dislikes, recent purchases, age, gender and other relevant demographic information the third party list developer feels is valuable. Also generally included on these forms is a check box which is either *already checked* or is unchecked when the individual enters the form. Depending on the status of the check box, a message next to the check box will read something along the lines of 'By checking this box I hereby authorize [Excite or other domain name] to use for its own purposes or distribute my personal information to third parties. I also would like to receive email regarding promotions/products that I may be interested in.

See Kline Aff. ¶ 25 and Exh. 33 (MonsterHut's Memorandum of Law in Support of Motion for a Preliminary Injunction, at 4, undated, filed in PaeTec Litigation) (emphasis added).

In sum, Hartl's admission, combined with MonsterHut's repeated concessions in filed

Memoranda of Law, as well as the Fourth Department decision, establish on the facts that its lists are not all permission based /opt-in, and that its representations to consumers to the contrary have been plainly false.

ARGUMENT

I.

RESPONDENTS REPEATEDLY HAVE VIOLATED GBL §§ 349 AND 350, EACH OF WHICH IS ACTIONABLE UNDER EXECUTIVE LAW § 63(12)

The Attorney General is proceeding under New York's Executive Law § 63(12), designating this a Special Proceeding, and seeking the plenary, broad injunctive relief that section permits. Section 63(12) is specifically designed to provide an expeditious means for the Attorney General to enjoin a wide range of illegal, fraudulent, or deceptive conduct, including Monsterhut's misrepresentations to consumers regarding the nature of their email lists, and how they collected them.

The Attorney General may bring a special proceeding under § 63(12) against any person or business that commits repeated or persistent "fraud or illegality" in transacting business. "It is well settled that . . . proof of scienter is not necessary" to establish a violation under Executive Law § 63(12). Lefkowitz v. Bull Investment Group, Inc., 46 A.D.2d 25 (3d Dep't 1974), appeal denied, 35 N.Y.2d 647 (1975). Further, the terms "fraud" and "illegality" are both broadly defined under the statute. Section 63(12) defines "fraud" as:

any device, scheme or artifice to defraud and any deception,
misrepresentation, concealment, suppression, false pretense, false promise
or unconscionable contractual provisions.

This definition goes well beyond that of common law fraud. In People v. Federated Radio Corp., 244 N.Y. 33, 38-39 (1926), the Court of Appeals emphasized:

In a broad sense the term [fraud] includes all deceitful practices contrary to the plain rules of common honesty The words "fraud" [or "fraudulent"] in this connection, should therefore be given a wide meaning, so as to include all acts, although not originating in any actual evil design or contrivance to perpetrate

fraud or injury upon others, which do by their tendency to deceive or mislead the purchasing public come within the purpose of the law.

Accord Bull Investment, 46 A.D.2d 25. It is well settled that violations of NY GBL § 349, which prohibits “deceptive acts or practices in the conduct of any business,” are remediable by the Attorney General in a § 63(12) proceeding. See People v. Allied Marketing Group, Inc., 220 A.D.2d 370 (1st Dep’t. 1995); People v. Lipsitz, 174 Misc. 2d 571 (Sup. Ct. N.Y. Co. 1997) (enjoining under Executive Law § 63(12) and GBL §§ 349-350 defendant’s use of deceptive emails and the Internet, to falsely advertise phony magazine subscriptions which either never arrived or were extremely delayed).⁵

Respondents’ conduct likewise constitutes “illegality” under Executive Law § 63(12). The term “illegality” within the meaning of Executive Law § 63(12) refers to the repeated violation of any law or regulation, whether promulgated by the federal government, by the State of New York -- such as GBL §§ 349-350 or by one of its political subdivisions. See generally State of New York v. Princess Prestige, 42 N.Y.2d 104 (1977); Lefkowitz v. E.F.G. Baby Products, 40 A.D.2d 364 (3d Dep’t 1973); People v. Anderson, 137 A.D.2d 259 (4th Dep’t 1988); State of New York v. Scottish-American Ass’n, 52 A.D.2d 528 (1st Dep’t 1976), appeal dismissed, 39 N.Y.2d 1057 (1976).

A. Respondents’ Conduct Violates GBL § 349

GBL § 349(a) provides that “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared

⁵ Accord People v. Emyre Inground Pools, Inc., 227 A.D.2d 731, 733 (3d Dep’t 1996); Lipsitz, 174 Misc. 2d 571; State of New York v. British & American Casualty Co., 133 Misc. 2d 352 (Sup. Ct. N.Y. Co. 1986).

unlawful.” The definition of deceptive practices under GBL § 349 is given parallel construction to that of fraud under Executive Law § 63(12). State of New York v. Colorado State Christian College, 76 Misc.2d 50 (Sup. Ct. N.Y. Co. 1973). GBL § 349(b) specifically authorizes the Attorney General to seek an order enjoining the continuance of deceptive practices and granting restitution to injured consumers, and GBL § 350-d provides for a \$500.00 penalty for each violation of §§ 349 and 350.⁶

Furthermore, when acting under § 349 and Executive Law § 63(12), it is unnecessary for the Attorney General to establish actual, present harm to specific consumers; rather, it is sufficient that a company has made deceptive claims – as Monsterhut has in this case. See Lipsitz, 174 Misc. 2d at 580 (“the Attorney-General's mandate is sufficiently broad that the Attorney-General could commence enforcement actions even if no complaints were to exist”); State of New York v. Management Transition Resources, Inc., 115 Misc. 2d 489, 490-91 (Sup. Ct. N.Y. Co. 1982) (where respondent makes “deceptive and hence unlawful” claims, “[i]t is not necessary for the Attorney-General to await consumer complaints before proceeding to enjoin this chicanery”).

In this case, the respondents undoubtedly have engaged in deceptive practices under § 349, as well as persistent and repeated fraudulent conduct under Executive Law § 63(12). From March 2001 to May 2002, respondents sent more than one-half billion unsolicited commercial emails on behalf of more than 130 different clients. Kline Aff., Exh. 4. During that period, respondents falsely described the lists containing consumer email addresses to

⁶ The meaning of deceptive practices under GBL §349 is given parallel construction to that of fraud under Executive Law § 63(12). Colorado State Christian College, 76 Misc. 2d at 54.

which it sent commercial email as, inter alia, “permission based,” and “100% percent permission based.” Kline Aff. ¶ 18. Respondent also falsely stated in commercial emails sent to consumers that its lists were “opt-in” lists. Kline Aff. ¶ 20. Additionally, in response to customer and consumer emails questioning whether MonsterHut’s commercial email was actually unsolicited, MonsterHut falsely replied that “[t]here is no question that your email address has been opted in” Kline Aff. ¶ 21. Yet while promising consumers that their lists were opt-in only, respondents were admitting in court that in fact, their lists included email addresses collected using both opt-in and opt-out protocols. Kline Aff. ¶¶ 24, 25 and referenced exhibits.

Respondents here have contested none of the specific allegations against them. In fact, they have admitted to most of the practices, in sworn testimony and memoranda in other litigation. See supra pp. 10-12. The evidence of their pattern of deception is overwhelming, in the form of both sworn affidavits, and numerous unsworn complaints. Kline Aff. ¶ 27.⁷ In short, this case is ripe for judgment, and as a matter of law and fact respondents’ pattern of abuse is well-established, fully documented, and beyond dispute.

B. Respondents’ Conduct Also Violates GBL § 350

GBL § 350-a prohibits false advertising, which it defines as advertising that is “misleading in a material respect,” either explicitly (by “statement, word, design, device, sound, or any combination thereof,” or by virtue of the “fail[ure] to reveal facts material in the

⁷ Even those complaints that were not in the form of a sworn affidavit are properly before this Court. New York’s courts consider consumers’ unsworn complaints in determining whether respondents have committed repeated and persistent fraudulent and illegal acts. See People v. Lipsitz, 174 Misc.2d 571 (Sup. Ct. N.Y. Co. 1997).

light of such representations with respect to the commodity to which the advertising relates . . .”⁸ The oft-repeated test is whether an advertisement has the “capacity” or “tendency” to mislead a consumer; moreover, the baseline test is not whether the “average man would be deceived,” but whether any, including “the ignorant, the unthinking and the credulous” would be. See, e.g., People v. Volkswagen of America, Inc., 47 A.D.2d 868 (1st Dept. 1975); State v. Abandoned Funds Information Ctr., Inc., 129 Misc.2d 614, 617 (Sup. Ct. N.Y. Co. 1985). As with deceptive business practices under GBL § 349, there is no scienter or intent element under GBL § 350. See Geismer v. Abraham & Strauss, 109 Misc.2d 495, 497 (Sup. Ct. Suffolk Co. 1981); Colorado State Christian College of Church of Inner Power, 76 Misc.2d at 56.

As detailed at length above, respondents sent more than one-half billion unsolicited commercial emails to consumers, Kline Aff., Exh. 4, while labeling the lists containing consumer email addresses to which they sent commercial email as “permission based,” “100% percent permission based,” “permission based . . . to the best of our knowledge,” and “opt-in.” See Kline Aff. ¶¶ 18, 20, and 21. These statements about the nature of their commercial emails are false and relate to the one aspect of commercial email that consumers consider most important: whether or not the consumer has solicited the email. There exists an obvious

⁸ In full, GBL § 350-a defines false advertising as:

advertising, including labeling, which is misleading in a material respect; and in determining whether any advertising is misleading, there shall be taken into account (among other things) not only representations made by statement, word, design, device, sound or any combination thereof, but also the extent to which the advertising fails to reveal facts material in the light of such representations . . .

distinction between permission based and unsolicited commercial email. Permission based email is necessarily more valued by consumers because they believe they can trust the source. Respondents' lies regarding whether consumers had requested the emails constitute, in turn, false advertising under § 350. Accord Lipsitz, 174 Misc. 2d 571 (enjoining under Executive Law § 63(12) and GBL §§ 349-350 defendant's use of deceptive emails and the Internet to advertise phony magazine subscriptions).

Accordingly, respondents have violated GBL §§ 349 and 350, and in doing so, also violated the "fraud" and "illegality" prongs of Executive Law § 63(12).

C. Respondent has Asserted No Valid or Even Cognizable Defenses

Respondents MonsterHut and Pelow do not contest that any of these statements described supra at pp. 8-9 herein were made.⁹ In fact, they concede that they have made "statements [about 'permission based' data] that may be construed as misleading." Affidavit by Todd Pelow In Opposition to Preliminary Injunction dated July 11, 2002 ¶ 18 ("Pelow Aff.").

However, respondents raise two defenses, submitted only in conclusory form (by Affidavit of Todd Pelow), and without any evidentiary support. First, they argue they should not be held liable for their statements that their email lists were "permission based" because the statements were true "to the best of [their] knowledge," Pelow Aff. at ¶ 18, 20, and because they simply relied on the "represent[at]ions" of "affiliates" when making these statements. Id.

⁹ In response to the Petition, respondent Pelow submitted an "Affidavit in Opposition to Preliminary Injunction" on behalf of himself and the corporate respondent. Respondent Hartl has submitted nothing. Pelow claims in the first of his three paragraphs each numbered "2" that Hartl will either answer independently or not at all.

See also id. ¶ 4 (citing unspecified “representations by those from whom the data was acquired”). On the law, this argument is simply a *non sequitur*, because intent is not an element under Executive Law § 63(12), or GBL §§ 349-350.¹⁰ On the facts, respondents’ statements are purely conclusory: they do not submit any evidence -- much less credible evidence -- of any so-called “affiliates” they relied on, or what the purported affiliates’ “representations” were, much less any supportive precedent. In short, respondents submit no legal or logical reason to excuse them from their representations, particularly if based on the unsupported defense that they made them without even checking or confirming their veracity.

Second, Pelow claims (again, without any documentary support) that the terms “permission based,” “opt-in,” and “opt-out” do not have “clearly defined” meanings. His sole support for this conclusory statement, in the face of a mountain of evidence that there are clearly defined meanings (see Kline Aff. ¶¶ 10-17), is his self serving observation that there are “various meanings to many types of email marketing and although there are some entities that agree on some of the terms they all clearly do not.” Pelow Aff. ¶¶ 9, 11, 25.

Pelow’s contention is as incorrect as it is conclusory, and it is belied by Monsterhut’s own statements in an unrelated case. First, Pelow offers no evidence to rebut the exhaustively detailed list of definitions provided in the Petition and supporting affirmation. Furthermore,

¹⁰ See Bull Investment Group, 46 A.D.2d at 28, (“It is well settled that the definition of fraud under [§63(12)] is extremely broad and proof of scienter is not necessary.”) (citations omitted), E.F.G. Baby Products, Inc., 40 A.D.2d 364 (“Respondent’s defense that it acted in good faith, even if believable, is irrelevant as to the question of the illegality of the act [pursuant to § 63(12)] and to the question of further violations.”); Abraham & Strauss, 109 Misc.2d at 496-497 (“It seems clear that the plaintiff need not prove intent to deceive to establish false advertising.”); Colorado State Christian College of Church of Inner Power, Inc., 76 Misc.2d at 56 (holding that just as “[f]ederal courts have consistently held that proof of intention to deceive is not requisite to a finding of a violation of the Federal Trade Commission Act,” the same standard must apply G.B.L. § 349, which is based on that Act).

MonsterHut's own Memorandum of Law, submitted in another litigation, acknowledges what Pelow now purports to doubt, namely that: "A permission based protocol is one in which consumers 'opt-in' . . ." Kline Aff. ¶ 19 and Exh. 18 (Memorandum of Law in Support of a Temporary Restraining Order and Preliminary Injunction at 4, dated Aug. 23, 2001, filed in MAPS Litigation.)

Where, as here, respondents have raised no hard (much less persuasive) evidence, only asserting conclusory statements, they have failed to raise an issue of triable fact, and thus the Petition should be granted. See generally State of New York v. Daro Chartours, 72 A.D.2d 872 (3d Dept. 1979).

II.

BECAUSE RESPONDENTS HAVE RAISED NO TRIABLE ISSUE OF FACT, THE PETITION MUST BE GRANTED AND NO HEARING IS REQUIRED

A special proceeding brought under Executive Law § 63(12) in the form of a Petition, is "plenary as an action, culminating in a judgment, but is brought on with the speed and inexpensiveness of a mere motion." Siegel, New York Practice § 547 (2d ed. 1991). The legislative purpose for allowing a special proceeding under Executive Law § 63(12) is plain: the public interest is well served by an expeditious means for the Attorney General to seek relief for victims of consumer fraud. People v. B.C. Associates, Inc., 22 Misc.2d 43 (N.Y. Co. 1959).

Article 4 of the CPLR requires that on the return date of such a Petition "[t]he court shall make a summary determination upon the pleadings, papers and admissions to the extent that no triable issues of fact are raised." CPLR § 409(b). The tests and standards applied to

decide whether a petition, answer, and affidavits create triable issues of fact are the same as those applied on a motion for summary judgment pursuant to CPLR § 3212. Lefkowitz v. McMillen, 57 A.D.2d 979 (3d Dept.), motion for leave to appeal denied, 42 N.Y.2d 807 (1977); State of New York v. Management Transition Resources, Inc., 115 Misc.2d 489 (N.Y. Co. 1982).

Thus, courts have regularly enjoined fraudulent and illegal conduct without requiring a trial. See People v. Allied Marketing Group, Inc., 220 A.D.2d 370 (1st Dept. 1995); People v. Helena VIP Personal Introduction Service of New York, Inc., 199 A.D.2d 186 (1st Dept. 1993).¹¹

By contrast, in order to defeat the Petition in a special proceeding under Executive Law § 63(12), respondents “must present facts having probative value sufficient to demonstrate an unresolved material issue which can be determined only at a plenary trial.” State v. Waterfine Water Conditioning Co. of New York, Inc., 87 Misc.2d 18, 19 (Sup. Ct. Albany Co. 1975). Where, as here, the Attorney General amply has supported his allegations, the burden – here wholly unmet – is on respondents to establish by “proof of an evidentiary nature, the existence of a triable issue.” State v. Midland Equities of New York, 117 Misc.2d 203, 207 (Sup. Ct. N.Y. Co. 1982).

General denials, insufficient documentation, conclusory statements and self-serving explanations such as those offered by respondents (see supra pp. 18-20) are insufficient to prevent judgment without trial. See Daro Chartours, 72 A.D.2d at 872; see also Helena VIP,

¹¹ Accord State v. Scottish-American Ass’n, Inc., 52 A.D.2d 528 (1st Dep’t), appeal dismissed, 39 N.Y.2d 1057 (1976).

199 A.D.2d at 186; McMillen, 57 A.D.2d at 979.

Respondents here have not submitted any credible or probative evidence, much less any documentation, to rebut the evidence submitted by the Attorney General. Instead, they assert only conclusory, unsupported denials, reliance on unspecified third parties and equally unspecified representations made to them, and legally irrelevant defenses, such as supposed lack of scienter. None of these comes close to raising any triable issues. See supra pp. 18-20.

By contrast, the Attorney General has submitted a mountain of undisputed evidence showing that:

- Respondents repeatedly claimed that they were not spammers, i.e., that their email lists were in fact “100% permission based” and “opt-in”;
- The Fourth Department has held as a matter of law that respondents are spammers;
- Even respondents themselves repeatedly have conceded in other proceedings that their lists are not 100 percent permission based, or opt-in;
- And finally, every authority cited in the record demonstrates that the terms “permission based” and “opt-in” have clearly defined, and widely accepted meanings – which without question exclude and render false respondents’ claims.

Accordingly, because the respondents have failed to rebut the evidence presented by the Attorney General, and merely made general denials and conclusory allegations, they have failed to meet their burden of raising a triable issue of fact, and thus, no hearing is required.

III.

THE ATTORNEY GENERAL IS ENTITLED TO INJUNCTIVE RELIEF, A PERFORMANCE BOND, PENALTIES AND COSTS

In cases under Executive Law § 63(12) and GBL §§ 349 and 350, the Court has broad

equitable authority to grant injunctive relief, damages, costs and civil penalties. Here, we ask the court to grant such relief to enjoin respondents, individually or collectively, from carrying on or resuming their deceptive practices, and awarding costs and penalties.

A. The Court Should Enjoin Respondents' Fraudulent and Illegal Conduct

Where the evidence supports the relief requested and there are no triable issues of fact, courts routinely grant permanent injunctive relief in cases brought pursuant to § 63(12). The courts' remedial powers under § 63(12) are extremely broad. See Princess Prestige Co., 42 N.Y.2d at 108; Daro Chartours., 72 A.D.2d 872; Scottish-American Assoc., 52 A.D.2d at 528; Midland Equities of New York, 117 Misc.2d at 203. The Court should permanently enjoin respondents from engaging in the fraudulent and illegal practices alleged and proved in this proceeding. People v. Compact Associates, 22 A.D.2d 129 (1st Dept. 1964); State of New York v. Person, 75 Misc.2d 252, 253 (Sup. Ct. N.Y. Co. 1973).

In addition, we respectfully request that the Court order the respondents to account for the origin of each of the consumer email addresses they employed, and to establish a notification procedure to consumers regarding this information, so that in the future consumers can make more informed decisions about when, where and to whom they share their email addresses.

B. Respondents Should be Ordered to Pay Penalties and Costs

GBL Article 22-A, § 350-d provides for the assessment of a civil penalty of up to \$500 for each deceptive act or false advertisement in violation of Article 22-A. Each of the respondents' advertisements constitutes a separate violation for purposes of assessing penalties, see, e.g., United States v. Readers Digest Ass'n, Inc., 662 F.2d 955, 956 (3d Cir. 1981)

(\$1,750,000 penalty based on some 17,000 misleading sweepstakes solicitations mailed).

The general principles governing the appropriate amount of a penalty for violation of a consumer protection statute are set forth in Meyers Bros. Parking Sys. v. Sherman, 87 A.D.2d 562, 563 (1st Dept. 1982), aff'd, 57 N.Y.2d 653 (1982). Namely, the penalty should not be so small as to represent merely a cost of doing business; to the contrary, the penalty must be large enough to serve as a warning to discourage the prohibited act. At the same time, the penalties imposed should not be "shocking to one's sense of fairness." Id. Here, a penalty based on the number of unsolicited bulk (as opposed to individual) mailings respondents sent --131 (see Kline Aff. ¶ 5 and Exh. 4) -- will serve as a warning to discourage this kind of wrongful conduct and is in no way shocking to anyone's sense of fairness. Under this approach, penalties of \$65,000 (based on a \$500 penalty for 131 mailings) against each respondent are well justified.

CPLR § 8303(a)(6) of the CPLR provides that the court may additionally award the Attorney General "a sum not exceeding two thousand dollars against each defendant" in a § 63(12) special proceeding. Courts have routinely granted these costs. See e.g., Daro Chartours., 72 A.D.2d at 873; Midland Equities of New York, 117 Misc. 2d at 208; Lefkowitz v. Therapeutic Hypnosis, 83 Misc.2d 1068 (Sup. Ct. Alb. Co. 1975), rev'd on other grounds, 52 A.D.2d 1017 (3d Dept. 1976). We therefore request that such costs be imposed here.

C. Respondents Should Be Ordered to Post a Performance Bond

In addition, the Court should permanently enjoin respondents from engaging in any email or Internet related business within the State of New York until a \$100,000 performance

bond is filed with the Attorney General by a surety or bonding company licensed by and in good standing with the New York State Department of Insurance. The posting of such a bond will guarantee that respondents comply with any injunction this Court issues and will insure that the public interest is protected. The granting of a performance bond is within the broad remedial injunctive powers of the Court. People v. Allied Marketing Group, 220 A.D. 2d 170 (1st Dep't 1995) (\$500,000 bond ordered); People v. Helena VIP Personal Introduction Service of New York, Inc., N.Y.L.J., 1/17/92, p.26 col. 3 (Sup. Ct. N.Y. Co.), aff'd, 199 A.D.2d 186 (1st Dep't 1993) (\$500,000 bond ordered); Empyre Inground Pools, 227 A.D.2d 731 (\$100,000 bond ordered).

IV.

THE INDIVIDUAL RESPONDENTS ARE PERSONALLY LIABLE FOR THE REPEATED AND PERSISTENT FRAUDULENT, DECEPTIVE AND ILLEGAL ACTS ALLEGED IN THE PETITION

Executive Law § 63(12) is directed against "any person" who "shall engage in repeated fraudulent or illegal acts." It is well-settled that corporate officers and directors are liable for fraud if they personally participate in the illegal or fraudulent acts or have actual knowledge of them. State of New York v. Apple Health and Sports Clubs, Ltd., Inc., 80 N.Y.2d 803, 807 (1992); Empyre Inground Pools, Inc., 227 A.D.2d at 734; People v. Concert Connection, Ltd., 211 A.D.2d 310, 310 (2nd Dep't 1995); Marine Midland Bank v. John C. Russo Produce, 50 N.Y.2d 31, 44 (1980). See also Lippman Packing Corp. v. Rose, 203 Misc. 1041 (N.Y. Mun. Ct. 1953) and cases cited therein. "Corporate officers are to be held accountable for fraudulent acts whether acting on behalf of the corporation or on their own behalf." In re McGrath, 7 B.R. 496, 498-99 (S.D.N.Y. 1980).

Officers and directors will also be held liable for the fraudulent or illegal practices of their corporations if they "directed and guided the corporation in matters of policy." Consumer Sales Corp. v. F.T.C., 198 F.2d 404, 407 (2d Cir.), cert. denied, 344 U.S. 912 (1952), "occupied policy making or directing positions during the period of the violations charged" Benrus Watch Co. v. F.T.C., 352 F.2d 313, 325 (8th Cir. 1965), cert. denied, 384 U.S. 939 (1966), or controlled the financial affairs of the corporation F.T.C. v. Amy Travel Service, Inc., 875 F.2d 564, 573 (7th Cir. 1989).

New York courts routinely have found individual corporate officers and directors personally liable under Executive Law § 63(12) in such circumstances. See, e.g. Apple Health and Sports Clubs, 80 N.Y.2d 803 (finding a substantial likelihood of success in special proceeding by the Attorney General to establish personal liability against individual health club president and 50% shareholder with actual knowledge of and participation in corporation's fraudulent and illegal business dealings). See also Empyre Inground Pools, Inc., 227 A.D.2d at 731.

Further, all of the relief that can be obtained against the corporate entity can be obtained against the principals, including injunctive relief, restitution, penalties, costs and the posting of a bond. See Apple Health and Sports Clubs, 80 N.Y.2d at 803; People v. Court Reporting Institute, 245 A.D.2d 564 (2d Dep't 1997); Empyre Inground Pools, 227 A.D. 2d at 731; People v. Concert Connection, Ltd., 211 A.D. 2d 310 (2d Dep't 1995); People v. 21st Century Leisure Spa International, Ltd., 153 Misc.2d 938, 944-45 (Sup. Ct. N.Y. Co. 1991).

A. Todd Pelow

Todd Pelow is the Chief Executive Officer of MonsterHut, Inc. Kline Aff. ¶ 7 and

Exhs. 8-13. As CEO, Pelow not only knew of MonsterHut's false representations to consumers, but repeated them in sworn statements to other courts. Kline Aff. ¶¶ 22, Exhs. 8, 9. In MonsterHut's suit against PaeTec Communications, Pelow swore that MonsterHut only sends out "high volume, targeted, permission based emails to individuals who have 'opted in' to receive said email." Kline Aff., Exh 8, ¶16; Exh. 9, ¶ 13. Pelow is also intimately knowledgeable about how and from whom MonsterHut obtains the email addresses in its database. Kline Aff. Exh. 8 ¶¶ 17-19. In addition to his knowledge of the sole issue in this case, Pelow was involved in a broad range of duties including negotiating contracts, Kline Aff. Exhs. 8, ¶¶ 77-82, and 12, and handling complaints from consumers and MonsterHut's Internet access provider, Kline Aff. Exhs. 10, ¶¶ 15-19, and 12.

B. Gary Hartl

Gary Hartl is the Chief Technical Officer of MonsterHut, Inc. Kline Aff. ¶ 8. As CTO, Hartl has overseen all of the targeted email sent out by MonsterHut since March 15, 2001, Kline Aff. Exh. 14 ¶ 10, and is intimately knowledgeable about how and from whom MonsterHut obtains the email addresses in its database, Kline Aff. Exh 14 ¶¶ 5, 7, 8, and 10. Hartl's responsibilities at MonsterHut include "the management and coordination of the entire MonsterHut.com network, oversight of all email campaigns and responsibility for the acquisition, maintenance, and administration (removal of stale, undeliverable/non-existent and/or 'removal request' emails) of the targeted email lists utilized by MonsterHut.com." Kline Aff. Exh. 14, ¶ 2.

Thus, Pelow and Hartl each not only knew of the illegal and fraudulent acts of the corporate respondent, but they were involved in the creation and execution of the scheme, and

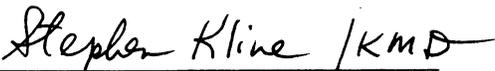
therefore should be held personally liable. All relief ordered against Monsterhut, Inc. therefore should be likewise ordered against these personally liable respondents, including penalties, injunctive relief, and the posting of a bond.

CONCLUSION

For the reasons set forth above, the Attorney General respectfully requests that the Court grant the relief sought in the accompanying Verified Petition, and such other and further relief that the Court deems necessary and appropriate.

Date: August 16, 2002
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