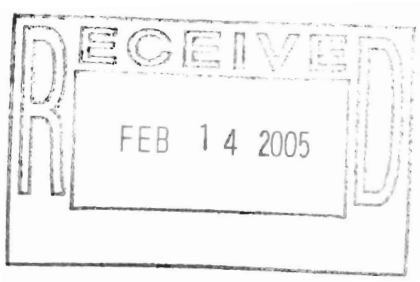
UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

OFFICE OF
THE COMMISSIONER



February 9, 2005

Dr. Paul Twomey
President/CEO
Internet Corporation for Assigned Names and Numbers (ICANN)
4676 Admiralty Way, Suite 330
Marina del Rey, California 90292-6601

6 Rond Point Schuman
Bt. 5
Brussels B-1040 Belgium

Dear Dr. Twomey:

I am writing to express concern about the problem of false domain name registration information maintained in the Whois database. This database is an essential tool for law enforcement agencies like the Federal Trade Commission and the Department of Justice, as well as law enforcers around the globe. But its effectiveness depends upon the accuracy of the underlying data. Although ICANN *requires* registrars to collect *accurate* contact information from website registrants, too often the actual data is incomplete or inaccurate, and therefore useless to law enforcement. I understand that ICANN, and its constituent organizations, is attempting to improve the Whois system; nevertheless, the FTC's recent action - - *FTC v. Global Net Solutions, Inc., et al.*, CV-S-05-0002-PMP (LRL) - - against the owners of several online pornography sites demonstrates that ICANN and the domain name registrars must do more. Simply put, domain name registrars have failed to ensure that the data they collect from registrants is accurate and ICANN has not exercised sufficient supervision over the registrars. At your earliest convenience, I would very much like to meet with you to discuss ways of improving the Whois system.

Since the advent of electronic commerce and the global online marketplace, the FTC has vigorously pursued law enforcement actions against online marketers and website operators engaged in deceptive or unfair business practices. Last year, the United States Congress also charged the Commission with enforcing the CAN-SPAM Act. This statute requires various identifying disclosures and expressly prohibits the use of deceptive information in connection with the transmission of unsolicited commercial email or "spam." Pursuant to the CAN-SPAM Act and Section 5 of the FTC Act, on January 3, 2005 the Commission filed a complaint in federal district court in Nevada against Global Net Solutions, Inc. and several individuals and related companies. The complaint alleges that the defendants bombarded consumers with millions of pieces of spam offering access to pornographic websites. In addition to links to the sites, many of the spam emails also contained actual pornographic images to which unsuspecting consumers were exposed when they opened the email.

As is often the case with FTC actions against illegal "spammers," as well as those engaged in other illegal online activities, deciphering the maze of interrelated companies and identifying and locating the individuals behind the Global Net business was difficult and very resource-intensive. Much of the purported contact data collected by the registrars - - Intercosmos Media Group (d/b/a directNIC.com) and DomainDiscover - - of the websites at issue in the *Global Net* case was false. For example, one of the individual defendants submitted both false name and address data while one of the named corporations falsely claimed to be located in Latvia. Commission investigators were eventually able to identify the individual defendants behind the websites but only after turning to alternative investigative tools. The delay caused by false Whois data is especially troubling where, as in *Global Net*, the alleged consumer harm is ongoing and unavoidable and the defendants are likely to destroy evidence and shield their assets from judgment.

The Commission's experience in *Global Net* highlights the serious deficiencies of ICANN's Whois system. Unfortunately, this experience is not unique. An informal sampling of Whois queries conducted by FTC staff in 2002 turned up numerous domain names with facially false address and contact information including websites registered to "God," "Bill Clinton," and "Mickey Mouse."[1] Indeed, the OECD's Committee on Consumer Policy has stated that the Whois system "cannot serve its functions if the data are incomplete or inaccurate" and has recognized that "[t]here remains room for improving the existing system." *Consumer Policy Considerations On The Importance Of Accurate And Available Whois Data*, June 2, 2003 pp. 6, 8.

Currently, ICANN's Registrar Accreditation Agreement requires registrars to collect accurate information from website registrants and, if a registrar is notified that the collected data is inaccurate, to "take reasonable steps to investigate the claimed inaccuracy." ICANN Registrar Accreditation Agreement, May 17, 2001, § 3.7.8. Registrars have discretion to cancel or suspend a domain name registered with inaccurate data. § 3.7.7.2. These requirements do not go far enough. ICANN must make registrars more accountable for the soundness of the data they collect from registrants. This includes not only the initial screening of data but also ongoing monitoring of data accuracy. It is insufficient for registrars to rely upon complaints from law enforcement agencies or injured consumers to alert them, after the fact, to the existence of false registration data. Moreover, in cases in which a registrant has repeatedly provided incomplete or inaccurate data, ICANN should *require* registrars to suspend or cancel domain registrations. Indeed, given the severity of the potential harm to children in situations in which the registered domain names are patently obscene - - some of the websites at issue in *Global Net*, for example, include names such as "f**k.com"[2] and "rapesex.com" - - ICANN should consider requiring registrars to exercise a higher degree of care in confirming the registrant's identity and location. Finally, ICANN should suspend registrars who repeatedly fail to collect accurate information.

---

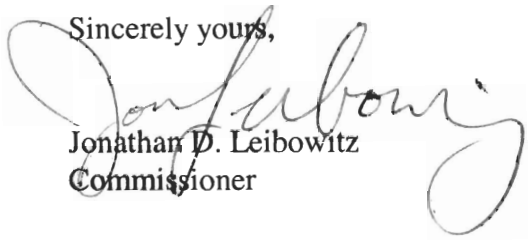
[1] Testimony of Federal Trade Commission Director of Bureau of Consumer Protection Director Howard Beales before Subcommittee on Courts, the Internet and Intellectual Property of the Committee on the Judiciary, United States House of Representatives, April 25, 2002.

[2] The asterisks are my own, the registered domain name was obscene.

I am sympathetic to the challenges ICANN and the registrars face in maintaining an accurate domain name registration system. Additional monitoring of registration data may impose costs on registrars, some of which are small companies that use automated registration procedures. If such costs are market-wide, however, their impact will be negligible. Further, concerns as to privacy and freedom of expression, while legitimate, are considerably lessened with respect to commercial registrants. In short, such challenges cannot serve as a justification for inadequacy.

If the promise of electronic commerce is to reach its true potential, ICANN and the registrars can and must do more to ensure that law enforcement agencies like the FTC are able to quickly identify commercial website operators that are engaged in fraud or other illegal activities. For your reference, I have attached a copy of the Commission's complaint in the *Global Net* matter.[3] I look forward to meeting with you and working to address these critical issues.

Sincerely yours,



Jonathan D. Leibowitz
Commissioner

---

[3] The views expressed in this letter are my own and do not necessarily reflect the views of the FTC or any other individual Commissioner.

cc:

Board of Directors
ICANN
4676 Admiralty Way, Suite 330
Marina del Rey, California 90292-6601

6 Rond Point Schuman
Bt. 5
Brussels B-1040 Belgium

Intercosmos Media Group, d/b/a directNIC.com
650 Poydras Street, Suite 1150
New Orleans, Louisiana 70130

DomainDiscover
PO Box 502010
San Diego, California 92150-2010

LAWRENCE HODAPP
STEPHEN L. COHEN
Federal Trade Commission
600 Pennsylvania Avenue, NW H-238
Washington, DC 20580
(202) 326-3105; 326-3222; 326-3395(fax)

BLAINE T. WELSH
Assistant United States Attorney
Bar No. 4790
333 Las Vegas Blvd. South, Suite 5000
Las Vegas, NV 89101
Phone (702)388-6336/fax(702)388-6787

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

Federal Trade Commission,

Plaintiff,

v.

Global Net Solutions, Inc., a Nevada corporation;

Global Net Ventures, Ltd., a United Kingdom company;

Wedlake, Ltd., a corporation;

Open Space Enterprises, Inc., a Nevada corporation;

Southlake Group, Inc., a Nevada corporation;

WTFRC, Inc., a Nevada corporation doing business as Reflected Networks, Inc.;

Dustin Hamilton, individually and as an officer or director of Global Net Solutions, Inc., Global Net Ventures, Ltd., and WTFRC, Inc.;

Tobin Banks, individually and as director of Open Space Enterprises, Inc.;

Gregory Hamilton, individually and as an officer and director of Southlake Group, Inc.;

Philip Doroff, individually and as an officer of Reflected Networks, Inc., now renamed WFTRC, Inc.; and

Paul Rose, individually;

Defendants.

CV-S-05-0002-PMP-LRL

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges as follows:

1. The Commission brings this action under Sections 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b) and 57b, and under Section 7(a) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM" or the CAN-SPAM Act), 15 U.S.C. § 7706(a), to obtain temporary, preliminary, and permanent injunctive relief, rescission of contracts, restitution, redress, disgorgement, and other equitable relief for Defendants' violations of Sections 5(a) and (d) of CAN-SPAM, 15 U.S.C. §§ 7704(a) and (d), the FTC's Adult Labeling Rule (the "Adult Labeling Rule" or the "Rule"), 16 C.F.R. Part 316.1, and Section 5 of the FTC Act, 15 U.S.C. § 45(a).

JURISDICTION AND VENUE

2. Subject matter jurisdiction is conferred upon this Court by 15 U.S.C. §§ 45(a), 53(b), 57(b), and 7706(a), and 28 U.S.C. §§ 1331, 1337(a), and 1345.

3. Venue in the United States District Court for Nevada is proper under 15 U.S.C. § 53(b) and 28 U.S.C. §§ 1391(b), (c), and (d)

PLAINTIFF

4. Plaintiff, the FTC, is an independent agency of the United States Government created by statute. See 15 U.S.C. § 41 et seq. The Commission enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits deceptive or unfair acts or practices in or affecting commerce. The FTC is also charged with enforcing various provisions of CAN-SPAM as if the violation of CAN-SPAM "were an unfair or deceptive act or practice proscribed under Section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))." 15 U.S.C. § 7706(a). The Commission is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and to secure such other equitable relief as may be appropriate in each case, including redress and disgorgement. 15 U.S.C. § 53(b).

DEFENDANTS

5. Defendant Global Net Solutions, Inc. ("GNS") is a Nevada corporation with its registered office located at 3960 Howard Hughes Parkway, Fifth Floor, Las Vegas, NV 89109. Since January 1, 2004, GNS has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. GNS resides in the District of Nevada and transacts business within the District of Nevada and throughout the United States.

6. Defendant Global Net Ventures, Ltd. ("GNV") is a United Kingdom company with its registered office located at Almeda House, 90-100 Sydney Street, London SW3 6NJ England. Since January 1, 2004, GNV has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. GNV transacts business within the District of Nevada and throughout the United States.

7. Defendant Wedlake, Ltd. ("Wedlake") purports to be a limited liability company allegedly located in Riga, Latvia. Since January 1, 2004, Wedlake has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. Wedlake transacts business within the District of Nevada and throughout the United States.

8. Defendant Open Space Enterprises, Inc. ("Open Space") is a Nevada corporation with its registered office located at 7311 S. Eastern Avenue, #281, Las Vegas, NV 89119. Since June 24, 2004, Open Space has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. Open Space resides in the District of Nevada and transacts business within the District of Nevada and throughout the United States.

9. Defendant Southlake Group, Inc. ("Southlake") is a Nevada corporation with its registered office at 6330 South Pecos Road, Suite 100, Las Vegas, NV 89120. Since January 1, 2004, Southlake has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. Southlake resides in the District of Nevada and transacts business within the District of Nevada and throughout the United States.

10. Defendant WTFRC, Inc., doing business as Reflected Networks, Inc. ("Reflected Networks"), is a Nevada corporation with its registered office located at 3960 Howard Hughes Parkway, Fifth Floor, Las Vegas, NV 89109, and a business address of 6363 South Pecos Road,

Las Vegas, NV 89120. On November 12, 2004, the corporation Reflected Networks, Inc. changed its name to WFTRC, Inc. Since January 1, 2004, Reflected Networks has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. Reflected Networks resides in the District of Nevada and transacts business within the District of Nevada and throughout the United States.

11. Defendant Dustin Hamilton ("D. Hamilton") is an officer of GNS, a director of GNV, and an officer of Reflected Networks He also uses the name "Donnie Gangsta" and the email address "donnie@signup4cash.com." Since January 1, 2004, he has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. He resides in the District of Nevada and transacts business within the District of Nevada and throughout the United States.

12. Defendant Tobin Banks ("Banks") is a director of Open Space. Since January 1, 2004, he has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. He resides in the District of Nevada and transacts business within the District of Nevada and throughout the United States.

13. Defendant Gregory Hamilton ("G. Hamilton) is an officer and director of Southlake. Since January 1, 2004, G. Hamilton has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. G. Hamilton resides in Tennessee and transacts business within the District of Nevada and throughout the United States.

14. Defendant Philip Doroff ("Doroff") was an officer of Reflected Networks, Inc., now renamed WTFRC, Inc., during 2004. Since January 1, 2004, he has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. He resides in Minnesota and transacts business within the District of Nevada and throughout the United States.

15. Defendant Paul Rose ("Rose") is an individual residing in Arizona. He also uses the name "john baker" and the email address "idbud@epimp.com." Since January 1, 2004, he has formulated, directed, controlled, or participated in the acts or practices set forth in this complaint. Rose transacts business within the District of Nevada and throughout the United States.

COMMON ENTERPRISE

16. Defendants GNS, GNV, Wedlake, Open Space, Reflected Networks, Southlake, D. Hamilton, Banks, Doroff, G. Hamilton, and other persons not named herein have operated and functioned as a single business enterprise in commission of the violations of the FTC Act, the CAN-SPAM Act, and the Adult Labeling Rule described below. They are referred to jointly in this Complaint as the "GNS Defendants."

17. Because each of the GNS Defendants functioned as a single business enterprise with the other Defendants in the commission of the law violations alleged above, they have each violated the CAN-SPAM Act, 15 U.S.C. §§ 7701 *et seq.*, the Adult Labeling Rule, 16 C.F.R. § 316.1(a)(1), and the FTC Act, 15 U.S.C. § 45(a).

COMMERCE

18. At all times relevant to this complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFINITIONS

19. **"Electronic mail message"** (or **"email"**) means a message sent to a unique electronic mail address. 15 U.S.C. § 7702(6).

20. **"Electronic mail address"** means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the "local part") and a reference to an Internet domain (commonly referred to as the "domain part"), whether or not displayed, to which an electronic mail message can be sent or delivered. 15 U.S.C. § 7702(5).

21. **"Commercial electronic mail message"** means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including the content on an Internet website operated for commercial purposes). 15 U.S.C. § 7702(2).

22. **"Affirmative consent"** to receipt of a commercial email message means that:

(A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative, and (B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages. 15 U.S.C. § 7702(1).

23. **"Header information"** means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message. 15 U.S.C. § 7702(8).

24. **"Initiate,"** when used with respect to a commercial email message, means to originate or transmit such message or to procure the origination or transmission of such message. 15 U.S.C. § 7702(9).

25. **"Procure,"** when used with respect to the initiation of a commercial email message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf. 15 U.S.C. § 7702(12).

26. "**Protected computer**" means a computer which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States. 15 U.S.C. § 7702(13); 18 U.S.C. § 1030(e)(2)(B).

27. "**Sender**" means a person who initiates a commercial electronic mail message and whose product, service, or Internet website is advertised or promoted by the message. 15 U.S.C. § 7702(16).

28. "**Sexually oriented material**" means any material that depicts sexually-explicit conduct as that term is defined in 18 U.S.C. § 2256, unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.

15 U.S.C. § 7704(d)(4). Sexually-explicit conduct is defined by 18 U.S.C. § 2256 to mean actual or simulated:

A. sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

B. bestiality;

C. masturbation;

D. sadistic or masochistic abuse; or

E. lascivious exhibition of the genitals or pubic area of any person.

DEFENDANTS' BUSINESS PRACTICES

29. Since January 1, 2004, and continuing to the present, Defendants have initiated the transmission of commercial email messages to protected computers. The primary purpose of these commercial email messages has been the commercial advertisement or promotion of Internet websites operated for a commercial purpose by the GNS Defendants.

30. Among the Internet websites operated for a commercial purpose by the GNS Defendants are at least a dozen content websites offering sexually oriented material. The GNS Defendants collect payment for viewing or access to this sexually oriented material through a payment site, which they also control: onlinecharges.com.

31. The GNS Defendants promote their websites through several methods, including an affiliate program offered on their website signup4cash.com. The GNS Defendants' affiliate program offers payments to third parties who steer consumers to the GNS Defendants' paid-content websites, including the websites, livewebfriends.com and livenetfriends.com. These third-party affiliates sometimes operate their own Internet websites that in turn link to the GNS Defendants' websites. The affiliates' websites most often are identified by hyperlinks in their email messages which also serve the purpose of identifying the affiliate deserving payment when a potential customer clicks through to Defendants' payment or content websites. Defendant Rose is an affiliate of the GNS Defendants, and his emails promoting the GNS Defendants' websites contain hyperlinks to websites registered by Rose, including bjkandy.com, jgjenny.com, fritzwebcam.com,

heheamber.com, hijenny.com, jnpage.com livejen.com, loljen.com, lolkandy.com, pkjen.com, profilejen.com, rrrjen.com, seetheprofile.com, starjen.com, tiffhuh.com, vgjen.com, wowjen.com, wtfjen.com, and xowebcam.com.

32. Defendants are "initiators" with respect to an email message when they have either originated or transmitted a message themselves or have procured the origination or transmission of a message through payments or other consideration, or inducements, to their affiliates.

33. The GNS Defendants are "senders" with respect to an email message when they have initiated a message and it is the GNS Defendants' websites that are being advertised or promoted by such message.

34. In numerous instances, the GNS Defendants have barraged consumers with emails containing sexually-explicit content. Defendants have initiated commercial email messages that include sexually oriented material to consumers who did not give prior affirmative consent to receipt of the messages. In numerous instances, these email messages fail to include the mark "SEXUALLY-EXPLICIT: " in the subject line of the messages, fail to include the mark "SEXUALLY-EXPLICIT: " and all required notices in the initially-viewable content of the messages, or fail to exclude sexually oriented material from the initially-viewable content of the messages.

35. In numerous instances, to induce consumers to open and read their commercial emails, Defendants have initiated commercial email messages containing materially false or misleading header information. In many instances, the email contains an originating email address that was not assigned by the email service provider. In other instances, the originating email address either was obtained through false representations to the email service provider that the email address would not be used to disseminate commercial emails or was used without the authorization of the subscriber who obtained the email address from the email service provider.

36. In numerous instances, to induce consumers to open and read their commercial emails, Defendants have initiated commercial email messages that contain subject headers that misrepresent the content or subject matter of the message. These emails include subject headers

that falsely represent that the email is a message from an internet service provider or a personal acquaintance of the recipient.

37. In numerous instances, consumers have been unable to stop the unwanted receipt of Defendants' commercial email because Defendants have sent the email messages without an "opt-out" mechanism; *i.e.*, the commercial emails have failed to contain a clear and conspicuous notice of the recipient's opportunity to decline to receive further email messages from Defendants and a functioning return email address or other Internet-based mechanism to accomplish such declination.

38. In numerous instances, Defendants have initiated commercial email messages to consumers who did not give prior affirmative consent to receipt of such messages and in those instances, failed to clearly and conspicuously identify the messages as advertisements or solicitations. Rather, Defendants routinely disguise their commercial emails by representing that their services are free.

39. In numerous instances, Defendants have initiated commercial email messages that failed to include a valid physical postal address of the sender.

VIOLATIONS OF THE ADULT LABELING RULE AND CAN-SPAM IN THE TRANSMISSION OF EMAIL THAT CONTAINS SEXUALLY ORIENTED MATERIAL

40. The Commission promulgated the Adult Labeling Rule pursuant to Sections 7704(d)(3) and 7711(a) of the CAN-SPAM Act, 15 U.S.C. §§ 7704(d)(3) and 7711(a). The Rule became effective on May 19, 2004, and sets forth marks and notices to be included in commercial email messages that contain sexually oriented material.

41. The CAN-SPAM Act and the Adult Labeling Rule both prohibit any person from initiating the transmission, to a protected computer, of any commercial email message that includes sexually oriented material and fails to include the phrase "SEXUALLY-EXPLICIT: " as the first nineteen (19) characters at the beginning of the subject line. 15 U.S.C. § 7704(d)(1)(A); 16 C.F.R. § 316.1(a)(1).

42. The CAN-SPAM Act and the Adult Labeling Rule also require that any message that includes sexually oriented material place only the following information within the content of the message that is initially viewable by the recipient, when the message is opened by the recipient and absent any further action by the recipient ("initially viewable content"):

A. the phrase "SEXUALLY-EXPLICIT: " in a clear and conspicuous manner, 15 U.S.C. § 7704(d)(1)(B)(i); 16 C.F.R. § 316.1(a)(2)(i);

B. clear and conspicuous notice that the message is an advertisement or solicitation, 15 U.S.C. § 7704(d)(1)(B)(ii); 16 C.F.R. § 316.1(a)(2)(ii);

C. clear and conspicuous notice of the opportunity of a recipient to decline to receive further commercial email messages from the sender, 15 U.S.C.§ 7704(d)(1)(B)(ii); 16 C.F.R. § 316.1(a)(2)(iii);

D. a functioning return email address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient may use to submit, in a manner specified in the message, a reply email message or other form of Internet-based communication requesting not to receive future commercial email messages from that sender at the email address where the message was received; and that remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message, 15 U.S.C. § 7704(d)(1)(B)(ii); 16 C.F.R. § 316 1(a)(2)(iv);

E. clear and conspicuous display of a valid physical postal address of the sender, 15 U.S.C. § 7704(d)(1)(B)(ii); 16 C.F.R. § 316.1(a)(2)(v); and

F. any needed instructions on how to access, or activate a mechanism to access, the sexually oriented material, preceded by a clear and conspicuous statement that to avoid viewing the sexually oriented material, a recipient should delete the email message without following such instructions, 15 U.S.C. § 7704(d)(1)(B)(iii); 16 C.F.R. § 316.1(a)(2)(vi).

43. The labeling and placement requirements of the CAN-SPAM Act and the Adult Labeling Rule do not apply if the recipient has given prior affirmative consent to receipt of the message. 15 U.S.C. § 7704(d)(2); 16 C.F.R. § 316.1(b).

44. Pursuant to Section 7711(a) of the CAN-SPAM Act, which allows the Commission to issue regulations to "implement the provisions of [CAN-SPAM]," and Section 7706(a), which provides that "[CAN-SPAM] shall be enforced by the [FTC] as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the [FTC Act] (15 U.S.C. 57a(a)(1)(B))," violations of the Adult Labeling Rule and Section 7704(d) of CAN-SPAM shall be enforced as if the violation were an unfair or deceptive act or practice proscribed under Section 18(a)(1)(B) of the FTC Act.

COUNT I

45. In numerous instances, the GNS Defendants have initiated the transmission, to protected computers, of commercial email messages that include sexually oriented material and that:

A. fail to include the phrase "SEXUALLY-EXPLICIT: " as the first nineteen (19) characters at the beginning of the subject line;

B. fail to include, within the initially viewable content of the message, a second instance of the phrase "SEXUALLY-EXPLICIT: ";

C. fail to include, within the initially viewable content of the message, clear and conspicuous notice of the opportunity of a recipient to decline to receive further commercial email messages from the GNS Defendants, or a functioning Internet-based mechanism that remains capable of receiving such requests for thirty (30) days;

D. fail to include, within the initially viewable content of the message, clear and conspicuous display of a valid physical postal address of the GNS Defendants; or

E. include sexually oriented material within the the subject line and/or the initially viewable content of the message.

46. In numerous instances, recipients of commercial email messages initiated by the GNS Defendants that include sexually oriented material have not given prior affirmative consent to receipt of such messages. In many cases, the messages say that they are from a party identified as a nonexistent electronic mail addresses, nonsense strings of characters, or random strings of names. Few, if any, recipients ever gave consent to receipt of messages from such parties or were given clear and conspicuous notice that any consent they gave to a different party could be transferred to the party identified as the source of the messages.

47. Therefore, the GNS Defendants' acts or practices violate Section 5(d) of the CAN-SPAM Act, 15 U.S.C. § 7704(d), and the Adult Labeling Rule, 16 C.F.R. § 316.1(a)(1).

VIOLATIONS OF THE CAN-SPAM ACT

48. The CAN-SPAM Act, 15 U.S.C. § 7701 et seq., became effective on January 1, 2004, and has since remained in full force and effect.

49. Section 5(a)(1) of CAN-SPAM, 15 U.S.C. § 7704(a)(1), states:

> It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading.

50. Section 5(a)(6) of CAN-SPAM, 15 U.S.C. § 7704(a)(6), states:

> For purposes of [section 5(a)(1)], the term "materially," when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic message or investigate the alleged violation.

51. Section 5(a)(2) of CAN-SPAM, 15 U.S.C. § 7704(a)(2), states:

> It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, if

such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the content or subject matter of the message (consistent with the criteria used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).

52. Section 7(e) of CAN-SPAM, 15 U.S.C. § 7706(e), states that in any action to enforce compliance through an injunction with Section 5(a)(2) and other specified sections of CAN-SPAM, the FTC need not allege or prove the state of mind required by such sections.

53. Section 5(a)(3) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(3), states:

> It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that –
>
> (i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and
>
> (ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

54. Sections 5(a)(5)(A) and (B) of the CAN-SPAM Act, 15 U.S.C. §§ 7704(a)(5)(A) and (B), state:

> (A) It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides –
>
> (i) clear and conspicuous identification that the message is an advertisement or solicitation;
>
> (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and
>
> (iii) a valid physical postal address of the sender.
>
> (B) Subpart (A)(i) does not apply to the transmission of a commercial electronic mail message if the recepient has given prior affirmative consent to receipt of the message.

55. Section 3(13) of the CAN-SPAM Act, 15 U.S.C. § 7702(13), defines "protected computer" by reference to 18 U.S.C. § 1030(e)(2)(B), which states that a protected computer is:

> a computer which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

56. Section 3(16) of the CAN-SPAM Act, 15 U.S.C. § 7702(16), defines "sender," when used with respect to a commercial electronic mail message, as:

> a person who initiates such a message and whose product, service, or Internet website is advertised or promoted by the message.

57. Section 7(a) of the CAN-SPAM Act states:

> [T]his Act shall be enforced by the [FTC] as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the [FTC Act] (15 U.S.C. 57a(a)(1)(B)).

COUNT II

58. In numerous instances, Defendants have initiated the transmission, to protected computers, of commercial email messages that contained, or were accompanied by, materially misleading header information, including but not limited to messages that included an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations;

59. Therefore, Defendants' acts or practices violate Section 5(a)(1) of CAN-SPAM, 15 U.S.C. § 7704(a)(1).

COUNT III

60. In numerous instances, Defendants have initiated the transmission, to protected computers, of commercial email messages that contained subject headings that would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.

61. Therefore, Defendants' acts or practices violate Section 5(a)(2) of CAN-SPAM, 15 U.S.C. § 7704(a)(2).

COUNT IV

62. In numerous instances, Defendants have initiated the transmission, to protected computers, of commercial email messages that advertised or promoted Defendants' Internet websites and failed to include:

A. clear and conspicuous notice of the recipient's opportunity to decline to receive further commercial electronic mail messages from Defendants at the recipient's electronic mail address; or

B. a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that remains capable for 30 days of receiving messages from the recipient requesting not to receive future commercial electronic mail messages from Defendants at the recipient's electronic mail address.

63. Therefore, Defendants' acts or practices violate Section 5(a)(3) or (5)(A)(ii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(3) or (5)(A)(ii).

COUNT V

64. In numerous instances, Defendants have initiated the transmission, to protected computers, of commercial email messages that failed to provide clear and conspicuous identification that the message was an advertisement or solicitation.

65. In numerous instances, recipients of the commercial electronic email messages set forth in paragraph 64 have not given prior affirmative consent to receipt of such messages. In many cases, the messages say that they are from a party identified as a nonexistent electronic mail addresses, nonsense strings of characters, or random strings of names. Few, if any, recipients ever gave consent to receipt of messages from such parties or were given clear and conspicuous notice

that any consent they gave to a different party could be transferred to the party identified as the source of the messages set forth in paragraph 64.

66. Therefore, Defendants' acts or practices violate Section 5(a)(5)(A)(i) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(A)(i).

COUNT VI

67. In numerous instances, Defendants have initiated the transmission, to protected computers, of commercial email messages that advertised or promoted Defendants' Internet websites and failed to include Defendants' valid physical postal address.

68. Therefore, Defendants' acts or practices violate Section 5(a)(5)(A)(iii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(A)(iii).

VIOLATION OF THE FTC ACT

69. As set forth below, Defendants, individually and in concert with others, have violated Section 5(a) of the FTC Act in connection with the marketing, promotion, offer, and sale of memberships in sexually-explicit Internet websites.

COUNT VII

70. In numerous instances, Defendants have represented, expressly or by implication, that Defendants will not charge consumers for memberships in their sexually-explicit Internet websites.

71. In truth and in fact, in numerous instances, Defendants charge consumers for memberships in their sexually-explicit Internet websites.

72. Therefore, Defendants' representation, as alleged in paragraph 70, is false and deceptive, and violates Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

INDIVIDUAL AND BUSINESS INJURY

73. Individuals and businesses throughout the United States have suffered, and continue to suffer, substantial injury as a result of Defendants' unlawful acts or practices. In addition,

Defendants have been unjustly enriched as a result of their unlawful practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

74. Sections 13(b) and 19(b) of the FTC Act, 15 U.S.C. §§ 53(b) and 57b(b), empowers this Court to grant injunctive and other relief to prevent and remedy Defendants' violations of the FTC Act, and in the exercise of its equitable jurisdiction, to award redress to remedy the injury to individuals and businesses, to order the disgorgement of monies resulting from Defendants' unlawful acts or practices, and to order other ancillary equitable relief. A violation of CAN-SPAM and the Adult Labeling Rule may be remedied in the same manner as a violation of the FTC Act. 15 U.S.C. § 7706.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff FTC, pursuant to Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b) and 57b, Section 7(a) of CAN-SPAM, 15 U.S.C. § 7706(a), and the Court's own equitable powers, requests that the Court:

1. Enter an order enjoining Defendants preliminarily and permanently from violating Section 5 of the FTC Act, the CAN-SPAM Act, and the Adult Labeling Rule, and freezing Defendants' assets;

2. Award Plaintiff such relief as the Court finds necessary to redress injury to any person and remove the benefits to Defendants resulting from Defendants' violations of the FTC Act, the CAN-SPAM Act, and the Adult Labeling Rule, including, but not limited to, rescission of contracts, restitution, redress, disgorgement of ill-gotten gains, and the refund of monies paid; and

3. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may deem just and proper.

Dated: January 3, 2005

Respectfully submitted,

JOHN D. GRAUBERT
Acting General Counsel

Lawrence Hodapp

Stephen L. Cohen
Attorneys for Plaintiff
Federal Trade Commission