

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FILED

MAY 16 2005

JUDGE AMY ST. EVE
United States District Court

FEDERAL TRADE COMMISSION,)
)
)
 Plaintiff,)
)
 v.)
)
 CLEVERLINK TRADING LIMITED, a)
 Cyprus limited liability company;)
)
 REAL WORLD MEDIA, LLC, a)
 California limited liability company;)
)
 BRIAN D. MUIR, individually, and as an officer)
 or director of Cleverlink Trading Limited;)
)
 JESSE GOLDBERG, individually, and)
 as an officer or director of Cleverlink)
 Trading Limited and Real World Media, LLC; and)
)
 CALEB WOLF WICKMAN, individually, and)
 as an officer or director of Cleverlink)
 Trading Limited and Real World Media, LLC,)
)
 Defendants.)
)

Case No. 05C 2889

Judge Amy J. St. Eve

Magistrate Judge Jeffrey Cole

**MEMORANDUM SUPPORTING PLAINTIFF'S *EX PARTE* MOTION FOR A
TEMPORARY RESTRAINING ORDER, OTHER EQUITABLE RELIEF, AND ORDER
TO SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE**

I. INTRODUCTION

Defendants are responsible for millions of “spam” e-mail messages that blatantly violate federal law and are causing significant injury to consumers and industry. The messages direct consumers to Defendants’ Web sites, which offer paid access to a membership site containing a purported database of lonely housewives looking for sexual encounters. At a minimum, Defendants’ use of illegal spam likely has generated hundreds of thousands of dollars in ill-gotten proceeds.

Defendants’ spam messages violate almost every provision of the CAN-SPAM Act, 15 U.S.C. § 7701, *et seq.* Defendants hide the origin of the spam by sending it through the computers of innocent third parties, and by forging information to make it appear that the messages were sent by third parties such as NASA. The spam often contains deceptive subject lines to fool consumers into opening messages they would otherwise delete. Some of the spam contains sexually explicit material without any warning or label, increasing the likelihood that the material will be viewed by children or by individuals at work. Finally, the spam does not provide consumers with an opportunity to opt-out of receiving future messages, and does not contain any valid contact information such as a postal address or an accurate return e-mail address. The FTC has received over 550,000 complaints about Defendants’ spam.

The purpose of the spam is to make money. The spam messages drive consumers to Web sites soliciting consumers to purchase access to the Defendants’ main membership site. The money that consumers pay for the membership site access goes directly to Defendants. In a four month period alone, Defendants took in nearly \$700,000 in membership fees.

In addition to sending spam that cannot be traced to the real sender, Defendants have taken other complicated steps to hide the fact that they run the spam operation. Defendants originally ran the operation using a company registered in their home state of California. However, after receiving numerous spam complaints, they undertook further efforts to hide their involvement. For example, Defendants have been using Web sites that are falsely registered to people in all corners of the world. Defendants also began using an offshore credit card processor, began using offshore bank accounts to collect ill-gotten spam proceeds, and began fronting the operation with a Cyprus company that they formed.

Taken as a whole, Defendants' actions appear purposefully calculated to avoid legal responsibility for their violations of CAN-SPAM. The FTC respectfully requests that this Court issue a TRO bringing Defendants' harmful and illegal scheme to a swift end. The FTC also requests that the TRO be issued *ex parte* and contain an asset preservation order to ensure that Defendants do not dissipate or transfer assets obtained from the illegal spam operation. Without the requested relief, Defendants' illegal spamming operation will continue unabated, and they are likely to conceal or dissipate assets and destroy records concerning their illegal activities.

II. JURISDICTION AND VENUE

This Court has subject matter jurisdiction over the FTC's claims pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345. Personal jurisdiction over Defendants is established pursuant to the FTC Act's nationwide service of process provision. *See* 15 U.S.C. § 53(b). "Where a federal statute provides for nationwide service of process, personal jurisdiction may be obtained over any defendant having minimum contacts with the United States as a whole." *FTC v. Bay Area Bus. Council, Inc.*, No. 02 C 5762, 2003 WL 1220245, at *2 (N.D. Ill. March 14, 2003); *see also United Rope Distribs., Inc. v. Seatriumph Marine Corp.*, 930 F.2d 532, 534 (7th Cir. 1991).

Venue is proper in the Northern District of Illinois. Pursuant to the FTC Act, an action may be brought where a corporation or person "resides or transacts business." *See* 15 U.S.C. § 53(b). Defendants have transacted considerable business in this district. ((*See* PX 3 ¶¶ 13, 15) (illegal e-mail messages routed through computers in this district); PX 1 ¶¶ 7-33 (FTC undercover purchases of Defendants' adult memberships from computer in Chicago); *id.* ¶¶ 46-47 (credit card processing records demonstrate Defendants have over 170 customers in this district)). Venue is also proper over Defendant Cleverlink Trading Limited because it is a foreign company which may be sued in any district. *See* 28 U.S.C. § 1391(d).

III. DEFENDANTS

Defendants are two companies and three individuals that operate as a common enterprise to market their Web sites with illegal spam messages. Although based in San Diego, Defendants have taken significant steps to hide their involvement such as employing false registration information for their Web sites, continually changing Web site addresses, using offshore banks, and fronting the operation with their Cyprus registered company.

A. The Companies

Defendants run their Internet business through two intertwined companies – Real World Media, LLC (“Real World”) and Cleverlink Trading Limited (“Cleverlink”). Real World is a California limited liability company. (PX 1 ¶ 43.) Cleverlink is a company formed under the laws of Cyprus. (*Id.* ¶ 41.) The spam operation was first run under Real World, but Defendants switched to Cleverlink after receiving numerous spam complaints. The switch appears to be simply for appearances, since the operation remains essentially the same. The companies share directors and shareholders, who reside in San Diego. (*Id.* ¶¶ 41, 43.) They share telephone numbers and a fax line. (*Id.* ¶¶ 46(m), 48(a), 48(i), 50(a-c).) The companies utilize the same online check processor to accept payment for memberships to the sites. (*Id.* ¶ 48(h).) Finally, the membership site that each company controls is essentially the same. (*Compare id.* ¶¶ 21-27, Att. B at OCW0019-25 with ¶¶ 9-16, 28-33, Att. A at WMB008-13 & Att. C at WOW007-12.)

1. The Spam Operation under Real World

Since early 2004, Defendants have employed spam e-mails to drive consumers to their Web sites, where consumers are encouraged to purchase access to Defendants’ membership site. Until about July 2004, this spam contained a hyperlink that, if clicked, directed consumers to one of many Web sites controlled by Real World. (PX 1 ¶¶ 21-27; 46(e-1); 50(a-e), 59(b), Att. N, at MSN E-mail 041-56 (examples of Real World spam).) Consumers who clicked on the hyperlink in the spam were sent to Web sites that solicited consumers to purchase access to Real World’s membership site. (*Id.* ¶ 46(g-i).) The site purports to offer a “data base” of “lonely house wives” seeking sexual encounters. (*Id.* ¶¶ 21-25, Att. B at OCW0000002, 19.) Real World utilized a credit card processor based in the U.S. to accept payments for memberships to its Web site. (*Id.* ¶ 46.) If consumers purchased a membership, Real World received the proceeds. (*Id.* ¶¶ 46(a-b), 52(b).) From April through July 2004 alone, Real World’s credit card processor paid Real World over \$690,000. (*Id.* ¶ 46(a).)

On several occasions between May and July of 2004, Real World’s credit card processor threatened to terminate Real World for “spamming” complaints. (PX 1 ¶ 46(e-1); 50(a-e).) In about July 2004, Defendants then switched the spam operation to be fronted by Cleverlink, a Cyprus company that they direct and own.

2. The Spam Operation After the Switch to Cleverlink

Since about July 2004, Defendants' spam has contained a hyperlink that, if clicked, directs consumers to one of many Web sites controlled by Cleverlink. (PX 1 ¶¶ 8-18, 28-33, 50(f-r), 51, 59(a, c, d) Att. N, at MSN E-mail 001-40, 057-75, 076-95, 096-119 (examples of Cleverlink spam).) Cleverlink registered dozens of these Web site addresses, but provided registration information that falsely identified the site owners as individuals in Venezuela, Chile, Argentina, and Greece. (PX 1 ¶¶ 50 (f-r), 54-55, Att. M at FTC000001-10.) The Web sites now direct consumers to a membership site controlled by Cleverlink. This site is substantively the same as the Real World membership site. (*See id.* ¶¶ 9-15, 51(a), Att. A at WMB0000008-13, Att. B at OCW0000019-25.)¹

Consumers that currently pay for Defendants' membership site by credit card have their payments processed by a company based in the Caribbean. (PX 1 ¶¶ 14, 28-31.) Additionally, records from Cleverlink's online check processor demonstrate that membership proceeds are now deposited into Cyprus accounts. (*Id.* ¶ 48(a, f, g, i).) In short, Defendants appear to have switched to Cleverlink solely to hide the fact that they run the operation and profit from the illegal spam.

B. Brian D. Muir

Muir is a director and shareholder of Cleverlink. (PX 1 ¶ 41(a, c).) Muir purchased a phone number used by both Cleverlink and Real World. (*Id.* ¶¶ 48(a), 49, 50(a-c), 51.) Muir also purchased an e-mail address used by Cleverlink for business purposes. (*Id.* ¶¶ 48(a, d, e, f, i), 49.) Muir has been described as the "technical contact" for Cleverlink. (*Id.* ¶ 48(h).)

C. Jesse Goldberg

Goldberg is a director and shareholder of Cleverlink and is the sole officer of a company that serves as one of two managers of Real World. (PX 1 ¶ 41(a, c), 43(b).) Goldberg signed a

¹ The FTC's undercover purchases of memberships reveal that this membership site does not provide a "database" of "lonely house wives." Instead, the site redirects members to an apparently unrelated general dating site. (See PX 1 ¶¶ 9-20, 28-37.) Further, the same access to this dating site can be otherwise obtained for free. (*Id.* ¶¶ 38-40.) Thus, Defendants' advertised "database" appears to be largely worthless.

contract with an online check processor for Cleverlink. (*Id.* ¶ 48(j).) Goldberg has communicated with Real World's credit card processor about its adult Web sites. (*Id.* ¶ 46(d).) Further, Goldberg purchased numerous domain names used by Real World, including the "spam" membership site. (*Id.* ¶ 50(a, d, e).)

D. Caleb Wolf Wickman

Wickman is a director and shareholder of Cleverlink and is the sole officer of a company that serves as one of two managers of Real World. (PX 1 ¶¶ 41(a), 43(a, b), 48(c).) Wickman signed a contract on behalf of Real World to process credit cards for Real World's adult Web site memberships (*id.* ¶ 46(m)), and he serves as a contact for Cleverlink's online check processor (*id.* ¶ 48(d, g, i)). Wickman has personally responded to spam complaints on behalf of Real World. (*Id.* ¶ 46(e-1).)

IV. DEFENDANTS' "SPAMMING" BUSINESS

As noted above, the sole purpose of the deluge of spam is to get consumers to buy access to Defendants' membership sites. Defendants are responsible for millions of commercial e-mail messages that blatantly disregard one or more of the protections Congress provided in the CAN-SPAM Act, 15 U.S.C. § 7701 *et seq.*, the federal law regulating commercial e-mail (discussed *infra* § V.B).²

Defendants' spam violates CAN-SPAM in several ways. The spam hides the identity of the sender, fools consumers into opening messages, fails to give consumers the ability to opt-out of further messages, and some messages contain sexually explicit language without a required label or warning. All of these illegal actions cause significant harm to consumers and Internet service providers. Since April 2004, consumers forwarded over 550,000 e-mail messages

² Congress passed CAN-SPAM after finding that spamming imposes significant costs on the e-mail system, which are passed along to subscribers in the form of higher prices and reduced convenience. *See id.* at §§ 7701(a)(3), (4). Congress found that unsolicited commercial e-mail messages – most of which are fraudulent or deceptive in one or more respects – threaten the convenience and efficiency of e-mail, an "extremely important and popular means of communication." *Id.* at §§ 7701(a)(1), (2). The law does not make all commercial e-mail illegal; it simply proscribes the most abusive practices. For example, it requires that commercial e-mail messages correctly identify their source, allow consumers to unsubscribe, and contain a physical postal address at which the recipient may contact the sender. *Id.* at § 7704.

advertising Defendants' Web sites to an e-mail address at which the FTC accepts spam complaints. (PX 1 ¶¶ 4, 56.) The spam continues to date. (*Id.* ¶ 61.)

A. Typical Spam Message

A typical spam message marketing Defendants' Web sites consists of a short text message or a picture and a hyperlink. (PX 1 ¶¶ 57-59, Att. N (examples of Defendants' spam); PX 2.) The text is often a purported message from a "lonely house wife" or an example of a purported "lonely house wife" profile supposedly contained in the "database" available on the Defendants' paid membership Web site. The e-mail itself contains a hyperlink that, if clicked, takes consumers to one of Defendants' numerous Web sites where a consumer can purchase access to the paid membership site. The FTC's investigation has revealed over 180 of these Web site addresses advertised in Defendants' spam. (PX 1 ¶¶ 53-55, Att. M at FTC0000001-10.) Defendants presumably cycle through those addresses in an attempt to evade filters aimed at detecting unwanted spam. (*Id.* ¶ 56.) The ever-changing, falsely registered domains also work to hide the fact that this is a single operation.

B. The Spam Falsifies Information That Would Identify the Real Sender

Defendants' spam messages employ at least three different illegal techniques to conceal the identity of the sender, a practice often referred to as "spoofing." (*See* PX 3 ¶¶ 6-7.) First, the messages include forged "from" and "reply-to" e-mail addresses that purport to identify who sent the e-mail. (*Id.* ¶¶ 3, 13, 16.)³ The "from" e-mail address in Defendants' spam often is comprised of random character strings such as SIEDNXTVWF@icqmail.com or kjuqrpefbk@hotmail.com. (*Id.*; PX 1 ¶¶ 57-60, Att. M at FTC0000010-11, Att. N.) Spammers blast out large volumes of e-mail hoping that some of it will reach a working e-mail address, and therefore much of the flow is not deliverable (*e.g.*, messages are sent to an account that is closed, full, or non-existent). The e-mail system returns undeliverable messages to the actual owner of the e-mail address, not the spammer. (PX 3 ¶ 8.) A large number of "bounced" e-mail flooding

³ An e-mail message typically consists of two parts, the header and the body. (PX 3 ¶¶ 3-4.) An e-mail "header" contains a variety of information – some of which is often visible to an e-mail recipient such as the "from" and "reply-to" fields. (*Id.*) Other e-mail information is often hidden, such as the Internet routing information of the message. (*Id.*)

back to the innocent party can wreak havoc on a computer system and cause significant problems. (*Id.*)

Second, Defendants' spam also often adds arbitrary, false routing information. (PX 3 ¶¶ 13, 17.) This information is meant to fool the computer system, and the e-mail recipient may not even see it. When e-mail messages are sent, they are routed through mail-exchanging computers. (*Id.* ¶ 4.) The computers that process and forward the e-mail messages insert a line of text that appears in the e-mail header as a "Received from" line which contains identifying information about the computer transmitting the message. (*Id.*) Defendants' spam contains arbitrary "Received from" lines inserted in the routing information that falsely identify the messages as being transmitted by computers operated by entities such as NASA, the U.S. Department of Defense, and Prudential Securities. (*Id.* ¶ 17.) In fact, the messages were not transmitted by these entities, and the false information was likely inserted to fool filters to trust the messages that would otherwise be identified as unwanted spam and deleted. (*Id.* ¶¶ 6-7, 17.)

Third, Defendants' messages are often routed through third party computers to disguise the true origination point of the message. (PX 3 ¶¶ 9, 13-14.) Relaying messages through vulnerable computers – many of which are simply personal computers with broadband connections operating without firewalls – is yet another way spammers can hide the origination point of spam. (*Id.* at ¶¶ 9-12.) Doing so obscures the routing information of the e-mail message by identifying the sending computer as the computer that was used as a relay, in effect "laundering" the message. (*Id.* ¶¶ 11-12.) Spammers typically use this method to evade anti-spam efforts of the spam recipient or his or her Internet service provider. (*Id.* ¶¶ 6, 9-10.) Such practices can cause real harm to users whose computers are unwittingly used as a relay. First, when functioning as a spam relay, a computer will often be slower than normal (or unstable and more likely to crash than normal). (*Id.* ¶ 10.) Moreover, if an individual's computer is repeatedly used as a launching pad to send spam, the user could be terminated by his or her Internet service provider if spam complaints are connected to the user's machine. (*Id.*)

C. The Spam Attempts to Fool People Into Opening the Messages

Consumers decide whether to open an e-mail message by reading the subject line of the message. The subject lines of many of Defendants' spam messages deceptively suggest that the

recipients have a prior personal relationship with the sender. The subject lines in the messages include: (1) “Hey, whats up?..,” (2) “just replying to your message,” and (3) “replying to your email.” (PX 1 ¶¶ 57-59, Att N at MSN E-mail047, 059, 063.) In truth, Defendants do not have prior relationships with the recipients (*see* PX 2 (e-mail messages sent to “trap” accounts)), and the subject lines are presumably used to trick consumers into opening messages that they otherwise would delete.

D. The Spam Contains Unlabeled Sexually-Explicit Content

Some of Defendants’ spam messages, when opened, reveal graphic sexually-explicit content. Many people do not wish to see such messages, but there is nothing in Defendants’ messages to alert consumers to the sexually explicit material. For example, opening some of the messages leads immediately to the following text:

- “My pussy gets wet when I see a guys cock. I really love oral sex, and would love to suck cock for hours, before he comes all over my face” Melissa (26, LA);
- “I never get enough sex from my partner, and I wish I could get fucked all day and night, I am looking for a lucky lover! I LOVE COCK!!!” Sarah (20, Texas); and
- “I love oral sex. My favorite position is 69 because there is nothing better in the world, then to feel a tongue on my wet and juicy pussy. I would love to suck your cock, till you cum on my titties.” Jen (25, Las Vegas).

(*See* PX 1 ¶¶ 57-59, Att. N at MSN E-mail001-040.) Subject headings and initially viewable sections of these messages bear no warning that the messages contain sexually explicit content, increasing the probability that such material will bypass filters and be viewed by children or by individuals at work.

E. The Spam Fails to Provide Consumers with an Opt-Out Mechanism

A key feature of CAN-SPAM is the requirement that commercial e-mails sent to consumers contain a mechanism that consumers can use to opt-out of receiving future e-mails. Defendants’ spam messages, however, fail to provide consumers with the opportunity to “opt-out.” First, many of Defendants’ spam messages do not include *any* notification to recipients of their ability to decline receiving further e-mail messages from Defendants. (*See, e.g.*, PX 1 ¶¶ 57-59, Att. N at MSN E-mail001-058.) Other messages contain possible opt-out links that are not clearly and conspicuously identified, providing hyperlinks identified with statements such as

“no more?” or “Forbid:.” (*See, e.g., id.* at MSN E-mail076, 81, 83.) Thus, once consumers receive unwanted messages, there is no mechanism by which consumers can stop the messages.

V. ARGUMENT

Defendants’ spamming operation violates almost every provision of the CAN-SPAM Act. They send out millions of illegal e-mail messages to consumers who, because of Defendants’ deceptive and illegal conduct, cannot stop the barrage of spam to their e-mail inboxes. Despite complaints about their spam that date back at least a year, the illegal spam has continued unabated. In order to protect the public from Defendants’ illegal activities and to prevent Defendants from continuing to make unlawful profits, the FTC requests that the Court enter a TRO with ancillary equitable relief to stop the illegal conduct immediately and to ensure that the Court can grant effective final relief at the conclusion of this case.

A. Injunctive Relief Standard

A district court may issue injunctions to enjoin violations of the FTC Act. *See* 15 U.S.C. § 53(b); *FTC v. Febre*, 128 F.3d 530, 534 (7th Cir. 1997); *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1028 (7th Cir. 1988). To obtain a temporary restraining order, the FTC must merely demonstrate: (1) a likelihood of success on the merits, and (2) that the balance of the equities tips in its favor. *World Travel*, 861 F.2d at 1029. “[T]he FTC need not prove irreparable injury to obtain a preliminary injunction.” *Kinney v. Int’l Union of Operating Eng’rs*, 994 F.2d 1271, 1277 (7th Cir. 1993). The threshold showing of a likelihood to succeed under the Seventh Circuit’s test for injunctive relief is a better than negligible chance of success on the merits. *See Cooper v. Salazaar*, 196 F.3d 809, 813 (7th Cir. 1999). Courts in this district have repeatedly exercised their authority to grant TROs in FTC actions. (*See infra* p. 15, n. 8; *see also* TRO Mot. at p.2, n.2.)

B. The FTC is Overwhelmingly Likely to Prevail on the Merits

The FTC alleges violations of the CAN-SPAM Act, 15 U.S.C. § 7701 *et seq.*, and the Adult Labeling Rule promulgated pursuant to the Act, 16 C.F.R. Part 316.4.⁴ These violations

⁴ The FTC Act prohibits “unfair or deceptive acts or practices.” 15 U.S.C. § 45(a). CAN-SPAM states that it “shall be enforced by the [FTC] as if the violation of this Act were an unfair or
(continued...)

are well-documented and widespread. Defendants are directly responsible for compliance with these laws and are directly liable for their systematic violation.

1. Defendants Are “Initiators” of Commercial E-mails

Defendants are legally responsible for the e-mail messages in this case. CAN-SPAM imposes liability for a commercial e-mail message upon “initiators” of the e-mail. 15 U.S.C. § 7704(a)(1). The definition includes not only those who “originate or transmit” the message, *i.e.*, the button pushers, but also those who “procure” the transmission of the message. 15 U.S.C. § 7702(9). CAN-SPAM defines procurers as those who “intentionally pay or provide other consideration to, or induce, another person to initiate” a message on their behalf. 15 U.S.C. § 7702(12). *See also FTC v. Phoenix Avatar*, No. 04C 2897, 2004 WL 1746698, at *13 (N.D. Ill. July 30, 2004) (“Liability [under CAN-SPAM] is not limited to those who physically cause spam to be transmitted, but also extends to those who ‘procure the origination’ of offending spam.”).

Here, Defendants “initiate” the commercial e-mail messages at issue. These e-mail messages direct consumers to Web sites that Defendants control (PX 1 ¶¶ 7-18, 28-33, 46(e-1), 59), and Defendants directly profit from traffic generated to their Web sites from the e-mail messages (*id.* ¶¶ 46, 48). Under these circumstances, it is axiomatic that either Defendants sent the messages themselves, or they procured someone to do it on their behalf. *See Phoenix Avatar*, 2004 WL 1746698, at *13 (granting preliminary injunction after finding it “quite likely” that the defendants who utilized Web sites to sell diet patches, and profited from those sites, “initiated the transmission of the spam advertising the Web sites”). Further, in responding to “spamming” complaints, Defendants have stated that e-mail messages marketing their Web sites are sent by “affiliates” or “advertisers” that they have the power to terminate. (PX 1 ¶¶ 46(e-1); 51(c-e).) As such, Defendants acknowledge that they procure others to send the illegal e-mail messages that market their Web sites.

⁴ (...continued)

deceptive act or practice proscribed under Section 18(a)(1)(B) of the [FTC] Act.” 15 U.S.C. 57a(a)(1)(B). A violation of a rule proscribed pursuant to 15 U.S.C. § 57a(a)(1)(B) is an “unfair or deceptive act or practice in violation of § 45(a)(1) [of the FTC Act].” *See* 15 U.S.C. § 57a(d)(3).

2. Defendants' Commercial E-mail Messages Violate CAN-SPAM

The evidence overwhelmingly shows that Defendants are violating CAN-SPAM. Defendants' commercial e-mail messages: (1) utilize false or misleading header information; (2) mislead recipients as to the nature of the e-mail through deceptive subject headings; (3) fail to include the opportunity to decline future e-mail messages; (4) fail to include the sender's postal address; and (5) violate the FTC's Adult Labeling Rule regarding sexually-oriented materials.

a. *False or misleading header information*

Defendants initiate commercial e-mail messages that contain "header information that is materially false or materially misleading" in violation of CAN-SPAM. 15 U.S.C. § 7704(a)(1).⁵ As described above in § IV.B, Defendants initiate commercial e-mail messages that contain forged "from" or "reply-to" e-mail addresses. The messages are routed through third parties' computers, falsifying the routing information of the message. The messages also contain arbitrary, false routing information. These techniques make it difficult, if not impossible, for consumers and law enforcement to determine the sender's true identity. By initiating spam containing materially false and misleading header information, Defendants violate CAN-SPAM.

b. *Deceptive subject headings*

Defendants initiate commercial e-mail messages that contain subject headings that are "likely to mislead a recipient . . . about a material fact regarding the contents or subject matter of the message" in violation of CAN-SPAM. 15 U.S.C. § 7704(a)(2). As demonstrated in § IV.C, subject headings of Defendants' spam like "Hey, whats up?" and "just replying to your message" deceptively suggest some sort of familiarity with the recipient of the e-mail. These headings in no way suggest that the message is an advertisement for a casual sex dating service and, therefore, violate CAN-SPAM.

⁵ CAN-SPAM defines "header information" as 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). For purposes of 15 U.S.C. § 7704(a)(1), "materially" includes "the alteration or concealment of header information in a manner that would impair the ability of . . . a law enforcement agency to identify, locate or respond to a person who initiated the e-mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message." 15 U.S.C. § 7704(a)(6).

c. *Failure to include opportunity to decline further e-mail messages*

Defendants initiate commercial e-mail messages that fail to include a “clear and conspicuous notice of the opportunity under [Section 5(a)(3)] to decline to receive further commercial electronic mail messages from the sender” in violation of CAN-SPAM. 15 U.S.C. § 7704(a)(5)(A). As discussed in § IV.E, Defendants violate this provision by either initiating messages that do not contain *any* mechanism at all to decline future e-mails, or by providing a mechanism that is obscured and therefore not clear and conspicuous.

d. *Failure to include a postal address*

CAN-SPAM requires that senders provide a physical postal address where the sender can be reached. *See* 15 U.S.C. § 7704(a)(5). A review of the e-mail messages demonstrates that Defendants fail to include a valid postal address in violation of CAN-SPAM. (*See* PX 1 ¶¶ 57-59, Att. N.)

e. *Violations of the Adult Labeling Rule*

Under CAN-SPAM, commercial e-mail that depicts “sexually explicit conduct,” as that term is defined in 18 U.S.C. § 2256, must include a label in its subject line, and exclude from the area “initially viewable to the recipient” sexual materials or anything other than specified items of information. 15 U.S.C. § 7704(d). Specifically, CAN-SPAM and the FTC’s Adult Labeling Rule prohibit any person from initiating commercial e-mail messages that include sexually oriented material and fail to include the phrase “SEXUALLY-EXPLICIT: ” as the first 19 characters at the beginning of the subject line. 15 U.S.C. § 7704(d)(1)(A); 16 C.F.R. § 316.4(a)(1).⁶ Here, as discussed in § IV.D, some of the Defendants’ e-mail messages contain graphic sexually-explicit content immediately viewable upon opening the e-mail messages. Defendants’ e-mail messages, however, do not contain the label “SEXUALLY-EXPLICIT: ”. (*See* PX 1 ¶¶ 57-59, Att. N at MSN E-mail001-040.)

3. **Muir, Goldberg and Wickman Are Individually Liable**

An individual may be held liable for corporate practices where he or she has authority to control the business affairs, such as by assuming the duties of a corporate officer, and has or

⁶ A main purpose of the Rule is to facilitate a mechanism by which consumers can filter out e-mails that contain sexually oriented material. *See* Label for Email Messages Containing Sexually Oriented Material, 69 Fed. Reg. 21,024, 21,024 (2004) (codified at 16 C.F.R. Part 316).

should have had knowledge of the deceptive practices of the business. *See FTC v. Amy Travel*, 875 F.2d 564, 573-74 (7th Cir. 1989); *see also World Travel*, 861 F.2d at 1031 (upholding freeze of individual assets). Here, as explained in § III.B, the individual Defendants are intimately involved in the affairs of the corporate Defendants and have direct knowledge of ongoing law violations. The individuals are corporate officers and directors, and they signed contracts and purchased various services to perpetuate the scheme. Indeed, as explained in § III.A, the individuals switched the spam operation from their U.S.-based company to a company formed under the laws of Cyprus after receiving numerous spam complaints. Rather than stop their illegal practices, it seems apparent that Defendants simply chose to take a series of extra steps to hide their involvement. Thus, injunctive relief is appropriate as to the individual Defendants.

C. The Balance of the Equities Favors the FTC

The balance of equities tips strongly in the FTC's favor. The FTC's Proposed TRO would prohibit Defendants and their agents from sending commercial e-mail messages that violate CAN-SPAM and preserve assets for equitable monetary relief. Without such relief, Defendants are free to continue collecting and spending profits from illegal activity throughout the pendency of this case. The TRO would work no valid hardship on Defendants, as they have no right to engage in, or profit from, practices that violate the law. In balancing equities, the Court must assign "far greater" weight to the public interest advanced by the FTC than to any of Defendants' private concerns. *World Travel*, 861 F.2d at 1030; *see also FTC v. Weyerhaeuser Co.*, 665 F.2d 1072, 1083 (D.C. Cir. 1981). The balance of equities also strongly favors the FTC because of the strong likelihood of success on the merits of its claims. *See Phoenix Avatar*, 2004 WL 1746698, at *15; *FTC v. Sabal*, 32 F. Supp. 2d 1004, 1009 (N.D. Ill. 1998).

D. The TRO Should Be Entered *Ex Parte* and Should Include Asset Preservation and Other Ancillary Relief

The FTC respectfully requests that this Court enter a narrowly tailored *ex parte* TRO that brings the Defendants' illegal practices to a swift end, and that preserves Defendants' assets in order to prevent ill-gotten gains from being dissipated or transferred. In fashioning appropriate injunctive relief, this Court has authority "to grant any ancillary relief necessary to accomplish complete justice[.]" *World Travel*, 861 F.2d at 1026; *see also Febre*, 128 F.3d at 534 (district

court has authority in FTC action to “order any ancillary equitable relief necessary to effectuate the exercise of the granted powers”). If a district court determines that it is probable that the FTC will prevail on the merits, the court has a “duty to ensure that the assets . . . [are] available to make restitution to injured consumers.” *World Travel*, 861 F.2d at 1031.

The FTC requests that the Court issue a TRO that provides for the following relief: (1) conduct prohibitions to ensure future compliance with CAN-SPAM, the Adult Labeling Rule, and the FTC Act (*see* Proposed TRO §§ I-VI); (2) asset retention, repatriation, and accounting provisions to preserve monies obtained unlawfully by Defendants (*see id.* §§ VII-XI, XIII); and (3) reporting and discovery provisions to obtain information relevant to a preliminary injunction hearing (*see id.* §§ VIII, IX, XII, XVII). These are necessary provisions which courts in this district have repeatedly granted to identify the scope of the unlawful practices, other participants, and the location of ill-gotten gains. (*See infra* p. 14, n. 8.) Defendants have no legitimate right to continue unlawful conduct, dissipate their unlawful profits or conceal information needed to effectuate relief in this case.⁷

Ex parte relief is necessary here. An *ex parte* TRO is warranted where facts show that irreparable injury, loss, or damage may result before defendants can be heard in opposition. *See* Fed. R. Civ. P. 65(b). Here, as in the other FTC actions in this district where courts have granted an *ex parte* TRO,⁸ there is a tangible risk that assets from the illegal activity, as well as relevant documents, will disappear if Defendants receive prior notice. Defendants have already

⁷ The FTC has submitted a Proposed Temporary Restraining Order with its papers.

⁸ Courts in this district have recently granted *ex parte* TROs under similar circumstances. *See, e.g., FTC v. Harry, et al.*, No. 04 C 4790 (N.D. Ill. Aug. 10, 2004) (Manning, J.) (granting *ex parte* TRO with asset freeze for violations of FTC Act and CAN-SPAM, order available over the Internet at <http://www.ftc.gov/os/caselist/0423085/040729tro0423085.pdf>); *FTC v. Phoenix Avatar LLC, et al.*, No. 04 C 2897 (N.D. Ill. April 23, 2004) (Holderman, J.) (granting *ex parte* TRO with asset freeze for violations of FTC Act and CAN-SPAM); *FTC v. Stuffingforcash.com, Inc.*, 02 C 5022 (N.D. Ill. July 16, 2002) (Norgle, J.) (granting *ex parte* TRO with asset freeze for violations of FTC Act for commercial e-mail marketing work-at-home scheme, order available over the Internet at <http://www.ftc.gov/os/2002/07/stuffingtro.pdf>); *FTC v. TLD Network Ltd.*, No. 02 C 1475 (N.D. Ill. Feb. 28, 2002) (Holderman, J.) (granting *ex parte* TRO with asset freeze for violations of FTC Act for commercial e-mail marketing deceptive sale of domain names, order available over the Internet at <http://www.ftc.gov/os/2002/03/1ldtro.pdf>). *See also* TRO Motion at p. 2, n.2.

demonstrated the ability to hide their identities. They use false addresses and routing information in their e-mail messages. They provide false registration information for Internet domain names that they purchase for their "lonely house wives" Web sites. Faced with complaints regarding spamming from their U.S. credit card processor, they began operating as a company from Cyprus, utilizing a bank account in Cyprus, and a credit card processor in the Carribean. In short, this is an operation set up specifically to avoid responsibility for the illegal actions it takes. The proposed order is aimed at preserving the status quo to ensure that Defendants cannot move assets and records outside of this Court's reach.⁹

VI. CONCLUSION

Defendants have caused and are likely to continue to cause injury and reap unjust enrichment because of their CAN-SPAM Act violations. Therefore, the FTC respectfully requests that this Court issue the requested injunctive and ancillary equitable relief to halt Defendants' illegal practices and ensure the availability of effective final relief.

Respectfully submitted,

William Blumenthal
General Counsel



Steven M. Wernikoff

Jason K. Bowler
Federal Trade Commission
55 E. Monroe St., Ste. 1860
Chicago, IL 60603
Voice: (312) 960-5634
Facsimile: (312) 960-5600

Dated: May 16, 2005

⁹ Although the extent of Defendants' ill-gotten gains from their activities is not known at this time (in part because assets are overseas), Defendants have received at least \$1.6 million from one payment processor that could be tied to illegal spamming. (PX 1 ¶ 46(a).) The FTC's Proposed TRO seeks an accounting of profits obtained or derived from commercial e-mail messages.