

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

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

SILI NEUTRACEUTICALS, LLC, and

BRIAN MCDAID, individually and doing
business as KAYCON LTD,

Defendants.

Case No. 07 C 4541

Judge David H. Coar

Magistrate Judge Morton Denlow

MICHAEL W. DOBBINS
CLERK, U.S. DISTRICT COURT

AUG 13 2007

FILED

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

I. INTRODUCTION

Defendants Brian McDaid and his company, Sili Neutraceuticals, LLC, deceptively market and sell dietary supplements on Internet Web sites utilizing a flood of illegal "spam" email messages. One of their products is a "human growth hormone" pill that Defendants claim reverses the aging process and causes users to look and feel 20 years younger. Another product is a diet pill purportedly made from an African plant called Hoodia gordonii that supposedly causes substantial weight loss. Analyses by medical experts, however, demonstrate that Defendants' product claims are completely baseless and that the products have no effect on users whatsoever. Since 2004, Defendants' false product claims have defrauded thousands of consumers out of over \$2.5 million, and their operation is ongoing.

To direct potential customers to the Web sites selling their products, Defendants employ massive amounts of illegal commercial email messages. The spam employs a pernicious new technique – the messages are transmitted through Internet Web site pages of innocent third parties. In addition to violating federal law by falsely identifying the true sender, the spam is

causing significant harm to individuals and companies who have had their Web sites hijacked. The spam violates the law in other ways, including by failing to offer any mechanism by which consumers can opt-out from receiving further email messages. Since July 2006, the FTC has received over 85,000 complaints about Defendants' spam.

The FTC respectfully asks this Court to bring Defendants' harmful practices to a swift end. The FTC brings this motion *ex parte* to obtain a temporary freeze of Defendants' assets in order to preserve the possibility of redress for victimized consumers who bought Defendants' products. Defendants have taken great efforts to cloak the responsibility for their illegal practices, utilizing different names, anonymous Web sites and spam. Moreover, they have transferred significant amounts of money to overseas bank accounts. Defendants' pattern of fraud, as well as their avid attempts to conceal their identity, indicates that they are likely to hide assets if they receive notice of this action.

II. JURISDICTION AND VENUE

The 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 defendants having minimum contacts with the United States as a whole." *FTC v. Bay Area Bus. Counsel, Inc.*, No. 02 C 5762, 2003 WL 1220245, at *2 (N.D. Ill. March 14, 2003).

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." 15 U.S.C. § 53(b). Defendants have transacted considerable business in this district. They have advertised and sold products to consumers in this district. (*See* PX 1 ¶¶ 6-19 (undercover purchases of Defendants' products in this district).) They also have utilized Internet services in this district. (*See* PX 1 ¶ 23, Att. Q; PX 6, Att. A (domain names purchased from domain name registrar located in this district); PX 12 (spam messages routed through Web site of organization located in this district).)

III. DEFENDANTS' ILLEGAL BUSINESS PRACTICES

Defendant Sili Neutraceuticals, LLC ("Sili") is a Nevada company that sells products on Internet Web sites. Defendant Brian McDaid ("McDaid"), a resident of Downingtown, Pennsylvania, is the sole officer of Sili. (See PX 1 ¶ 20, Att. O.)

Since early 2004 and continuing to the present, sales of Sili's products on its Web sites have generated over \$2.5 million. (PX 8 ¶¶ 3, 6.)¹ McDaid arranged for Sili to accept credit cards on its Web sites. (*Id.* ¶¶ 2-3, Att. A at CEN0013.) The credit card proceeds are deposited into a bank account opened by McDaid in the name of Sili. (*Id.* ¶ 3(B), Att. A at CEN0015; PX 9 ¶¶ 3-4.) Consumers who purchase Defendants' products receive them from a company identified as "Kaycon Ltd." (PX 1 ¶¶ 6-12, 13-19, Atts. F, M.) The labels on Defendants' products also identify the distributor as "Kaycon Ltd." (*Id.* ¶¶ 12, 19, Att. G at FTC046, Att. N at 076.) Kaycon is a company registered in the Caribbean (PX 17), and the Kaycon name is used by McDaid in his business (*see, e.g.*, PX 4 ¶ 3, Att. A at SER005).

Defendants' products appear to be marketed solely by commercial email messages. (PX 1 ¶¶ 6, 13, 30; PX 11 ¶ 17, Att. B (examples of email messages).) The email messages contain links that, if clicked, direct consumers to the Internet Web sites selling Defendants' products. (*Id.*; *see also* PX 11 ¶ 5 (explaining Internet domain names and Web sites).) The FTC has identified over 70 Web sites advertising Defendants' products; none of the Web sites identify Defendants as the seller or provide any contact information. (PX 1 ¶ 23, Att. Q.) McDaid purchased domain names for the Web sites. (*See* PX 1 ¶ 23, Att. Q; PX 6 ¶ 3, Att. A at INN007-8; PX 7 ¶ 5, Att. A at PAR003; PX 4 ¶¶ 2-3; PX 5 ¶¶ 3, 6.) The domain names were purchased using false names and addresses. (PX 1 ¶¶ 23-24, Att. Q.)

A. Defendants' False and Unsubstantiated Product Claims

Defendants deceptively market various herbal and "natural" products. They sell pills that supposedly elevate a user's level of human growth hormone under a variety of names, including "Dr-HGH" and "Perfect HGH" (collectively, "HGH Products"). (PX 1 ¶¶ 13-19, Atts. H-N.)

¹ From February through July 2004, Sili accumulated over \$480,000 in credit card sales using a credit card processor in Canada. (PX 8 ¶ 3(D), Att. A at CEN0018.) Since August 2004, Sili has utilized a credit card processor in the United States and generated over \$2.1 million in additional sales. (*Id.* ¶ 6.)

They also sell diet pills under a variety of names including “HoodiaHerbal” that purportedly contain Hoodia gordonii, a cactus-like plant found in Africa (collectively, the “Hoodia Products”). (*Id.* ¶¶ 6-12, Atts. A-G.) A single bottle of each of these products costs \$79.95 plus \$9.95 for shipping and handling. (*Id.* ¶¶ 8, 15.)²

1. Defendants deceptively promote their HGH Products

The Web sites and email messages promoting Defendants’ HGH Products make a variety of explicit claims about the products’ ability to turn back or reduce the aging process by altering the amount of human growth hormone in a user’s body. Email messages touting the products claim:

HGH [is] the only substance on earth proven by science to stall (and in many cases even reverse) the aging process, from wrinkles, to fat gain and muscle loss, to cellulite, to hair loss and decreased sexual libido/performance . . . this simple little pill causes your body to produce more natural HGH, after just a week or two of usage, and helps your body (and mind!) look and feel 5-10-15 years younger.

(PX 1 ¶ 13, Att. H; PX 11 ¶ 17, Att. B at MSN0032.) Defendants’ Web sites further claim that the HGH Products will make a user “look and feel 20 years younger” by causing a laundry list of positive effects on the body, including: (1) lowering blood pressure, (2) reducing cellulite, (3) improving vision, (4) causing new hair growth, (5) improving sleep, (6) improving emotional stability, (7) speeding injury recovery, (8) relieving chronic pain, (9) increasing muscle mass, and (10) causing fat and weight loss. (*See* PX 1 ¶ 14, Att. I at FTC049-55.)

Defendants’ claims about their HGH Products are false and unsubstantiated. In fact, according to a medical expert in endocrinology from Northwestern University, Defendants’ HGH Products have no effect on a person whatsoever. (*See* PX 2.) The products do not contain human growth hormone and cannot produce effects similar in nature to any form of growth hormone. (*See id.* ¶¶ 17, 27-28.)³ There is no credible medical evidence to support the claims

² In addition to the Hoodia Products and HGH Products, Defendants sell other herbal products touting weight loss and sexual virility. (*See* PX 1 ¶¶ 21, Att P.) The FTC has significant doubts that these other products are in any way effective and seeks injunctive relief in this matter aimed at prohibiting Defendants from making claims for any product unless they are true and Defendants can substantiate them with scientific evidence.

³ Human growth hormone (“GH”) is produced by the pituitary gland and is integral to the human growth process. (PX 2 ¶¶ 6-7.) In normal individuals, the production of GH naturally drops off

made by Defendants. (*Id.* ¶¶ 22, 25.) In sum, contrary to the claims made on their Web sites, Defendants' HGH products have no physiological effect on users. (*Id.* ¶ 27.)

2. Defendants deceptively promote and sell Hoodia Products

The Web sites and email messages promoting Defendants' Hoodia Products make extravagant weight loss claims, relying on purported scientific studies about the Hoodia gordonii plant. Most notably, Defendants claim that the Hoodia Products safely can cause as much as forty pounds of weight loss in a month. Email messages touting the products claim:

Hoodia is the most advanced (and by far the most successful) weight loss formula ever created, for one simple reason . . . it simply causes you to have less of an appetite, and eat less. Studies have proven time and time again that users of hoodia lose weight, an average of 1-3 pounds per week, but as high as 20-40 pounds a month in many participants.

* * *

There is no more effective product on the market, if you're looking to lose weight quickly yet SAFELY, and naturally . . . and the results speak for themselves, with over 94% of users reporting significant weight loss within the first two weeks of usage.

(PX 1 ¶ 6, Att. A at FTC002; PX 11 ¶ 17, Att. B at MSN044.) Defendants' Web sites make similar claims, stating, among other things: "[w]hat if you could actually shed 10, 15, or even 25 pounds quickly and safely in less than 30 days? Now you can[.]" (PX 1 ¶ 7, Att. B at FTC006.) Defendants further represent that the Hoodia Products will "keep the weight off permanently." (*Id.* ¶ at FTC009.)

Defendants' claims about their Hoodia Products are false and unsubstantiated. According to a medical expert in nutrition and obesity with Northwestern University's Feinberg School of Medicine, there is no credible medical evidence to support the claim that Hoodia gordonii (or any other ingredient in Defendants' Hoodia Products) causes weight loss. (PX 3 ¶ 14.) Furthermore, Defendants' claim that the Hoodia Products can cause users safely to lose 20 to 40 pounds a month is patently false because it is not safe or healthy to lose three pounds or more each week for several weeks. (*Id.* ¶ 19.) Given that the Hoodia Products do not cause weight

with the increase in age. (*Id.* ¶ 7.) The FDA has approved the use of a synthetic recombinant growth hormone, injected into the bloodstream, as a replacement for the body's own GH for individuals with an abnormal GH deficiency. (*Id.* ¶¶ 11-13.) Defendants' products, however, are tablets containing amino acids that, taken orally in the doses prescribed, have no effect on GH levels. (*Id.* ¶ 17.)

loss in the first place, their claim of permanent weight loss is also deceptive. (*Id.* ¶ 20.) Indeed, without a change in dietary or exercise habits, it is not feasible for users to experience permanent weight loss. (*Id.* ¶ 21.)

B. Defendants' Illegal Spamming Practices

Defendants likely are responsible for millions of illegal commercial email messages promoting their products. Since July 2006, consumers have forwarded over 85,000 email messages advertising Defendants' products to an email address at which the FTC accepts spam complaints. (PX 1 ¶ 23, Att. Q.) The FTC has submitted several examples of the spam as exhibits. (*See* PX 1 ¶ 25-26; PX 11 ¶ 17, Att. B.)⁴ All of the messages 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* § IV.B.2).⁵ The messages falsify information that would identify the real sender, contain false subject lines designed to fool people into opening the messages, and fail to include an opt-out mechanism by which consumers could stop the spam messages from continuing. These illegal actions cause significant harm to consumers and Internet service providers.

1. Defendants' spam falsifies information that would identify the real sender by routing the messages through innocent parties' Web sites

Defendants' email messages utilize a harmful new spamming technique aimed at hiding the identity of the true sender – the spam is blasted through vulnerable forms contained on Internet Web sites of innocent third parties. Web sites often contain forms that

⁴ The spam examples submitted were obtained by the FTC from a secure database run by Microsoft Corporation, which operates the free email service Hotmail. (PX 10.) The Microsoft database contains unsolicited email messages received by thousands of Hotmail "trap" accounts," *i.e.*, unused email accounts that receive unsolicited spam messages. (*Id.*)

⁵ Congress passed CAN-SPAM after finding that spamming imposes significant costs on the email 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 email messages – most of which are fraudulent or deceptive in one or more respects – threaten the convenience and efficiency of email, an "extremely important and popular means of communication." *Id.* at §§ 7701(a)(1), (2). The law does not make all commercial email messages illegal; it simply proscribes the most abusive practices. For example, it requires that commercial email 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.

allow users to do things like post comments, request a catalog or send a message to other Web site users (sometimes the forms contain titles like "Contact Us" or "Feedback Form"). (PX 11 ¶ 19; *see also* PX 12, Att. A (example of Web site form).) These forms usually contain various fields that can be filled in by the Web site visitor. (*Id.*) Users who fill in the form fields are invited to click a button to submit their information, and the message is then sent to the Web site operator.

Defendants' spam messages consistently are sent through third parties' Web site forms. (PX 11 ¶¶ 18, 22-24, Att. B.) Basically, the spam messages are injected into one or more fields of a vulnerable Web site form. (*Id.* ¶ 20.) When the Web site form is submitted, the injected spam message is delivered to multiple email addresses. (*Id.*)

This practice affects the ability to identify the true sender of the email message. The message appears to originate from the owner or operator of the Web site through which the spam is sent, rather than from the spammer's actual computer. (PX 11 ¶ 21.) In light of the fact that the email messages also fail to provide the physical address of Defendants, it is essentially impossible for a recipient of the email messages sent through the Web forms to identify the true sender of the message. (*Id.* ¶¶ 9-16, 21.)⁶

The costs to the victims of Web site form hijacking can be significant, as demonstrated by declarations from various victims. (*See* PX 12-16.) For example:

- the Save A Life Foundation, a nonprofit organization headquartered in Chicago that trains school children in first aid skills, had the form on its Web site hijacked in mid-June 2007, causing the organization to receive spam messages for Defendants' HGH Products to the email address at which it receives form inquiries, and forcing it to overhaul the exploited form (*see* PX 12);
- the owner of a limousine service in Northern California had a form on his Web site -- which served as the sole method by which customers could get quotes for his services -- hijacked to send spam for Defendants' products for months, resulting in the form being rendered useless and causing considerable lost business and complaints (*see* PX 13); and

⁶ In addition to cloaking the identity of the real sender, changing the address of the email message's return path causes harm to individual users and Internet service providers. When spammers send out email messages, a number of them are undeliverable because of wrong addresses or other reasons. (PX 11 ¶ 8.) The flood of undeliverable email messages is returned to the "reply-to" address of the innocent party, not the spammer, causing the innocent party and its Internet service provider to deal with additional bandwidth and transaction costs. (*Id.*)

- the Colorado State University's Office of Greek Life ("OGL") had a form on its Web site to give current and prospective members the ability to contact the office; during November 2006, spam messages touting Defendants' products were sent through the form resulting in complaints from consumers who received spam purporting to come from OGL, resulting in 40-50 hours of work to fix the Web site (*see* PX 14).

In short, sending the spam messages through hijacked Web sites passes real and substantial costs to innocent companies and individuals.

2. The spam attempts to fool people into opening the messages

Subject lines of email messages contain information that consumers use to evaluate whether to open the messages. The subject lines of many of the spam messages touting Defendants' products deceptively suggest that the recipients have a prior relationship with the sender. The messages include subject lines such as "Presagia Newsletter Subscription Request," "Re: hello," "Wineroom Contact Form," and "A comment from your personal blog." (PX 11 ¶ 17, Att. B at MSN0032, 47, 49, 68.) In fact, Defendants do not have prior relationships with the recipients (*see* PX 10 (email messages sent to "trap accounts")), and the subject lines presumably are used to trick consumers into opening messages they otherwise would delete.

3. The spam fails to provide consumers with an opt-out mechanism

A key feature of CAN-SPAM is the requirement that commercial email messages sent to consumers contain a mechanism that consumers can use to opt-out of receiving future messages. Defendants' spam messages, however, fail to provide consumers with the opportunity to opt-out. Indeed, Defendants' spam messages invariably do not include *any* notification to recipients of their ability to decline receiving further email messages from Defendants. (*See, e.g.*, PX 11 ¶ 17, Att. B.) Thus, once consumers receive unwanted messages, there is no mechanism by which consumers can stop the messages.

IV. ARGUMENT

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 an asset freeze and additional ancillary relief to ensure the availability of restitution to defrauded consumers. Courts in this district have repeatedly exercised their authority to grant TROs in similar FTC actions.⁷

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 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).

B. The FTC Is Overwhelmingly Likely to Prevail On the Merits

The FTC Act prohibits "unfair or deceptive acts or practices." 15 U.S.C. § 45(a). As shown above in Section III, the evidence clearly shows that Defendants have committed repeated violations of the FTC Act by making material misrepresentations to consumers about their products and have engaged in email practices that violate CAN-SPAM.

⁷ *See, e.g., FTC v. Kinion*, 05C 6737 (N.D. Ill. Dec. 7, 2005) (Hibbler, J.) (granting TRO and asset preservation for violations of CAN-SPAM Act); *FTC v. Cleverlink Trading Limited*, 05 C 2889 (N.D. Ill. May 15, 2005) (St. Eve., J.) (granting *ex parte* TRO and asset freeze for violations of CAN-SPAM Act); *FTC v. International Research & Dev. Corp. of Nevada*, 04C 6901 (N.D. Ill. Nov. 10, 2004) (Hibbler, J.) (granting TRO and asset preservation for violations of FTC Act and CAN-SPAM); *FTC v. Harry*, 04 C 4790 (N.D. Ill. July 27, 2004) (Manning, J.) (granting *ex parte* TRO and asset freeze for violations of FTC Act and CAN-SPAM); *FTC v. Phoenix Avatar LLC*, No. 04 C 2897 (N.D. Ill. April 23, 2004) (Holderman, J.) (granting *ex parte* TRO and 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 and asset freeze for violations of FTC Act concerning commercial email marketing work-at-home scheme); *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 email marketing deceptive sale of domain names).

1. Defendants' product claims are deceptive

Defendants' false claims about their products are "deceptive acts or practices" prohibited by Section 5 of the FTC Act. *See* 15 U.S.C. § 45(a). The FTC can establish corporate liability under Section 5 of the FTC Act by demonstrating "material representations likely to mislead a reasonable consumer." *FTC v. Bay Area Bus. Council, Inc.*, 423 F.3d 627, 635 (7th Cir. 2005); *see also* *FTC v. Phoenix Avatar*, No. 04 C 2897, 2004 WL 1746698, at *9 (N.D. Ill. July 30, 2004). The FTC is not required to prove intent to deceive. *Bay Area*, 423 F.3d at 635. The FTC may demonstrate the deceptive nature of advertising claims by either: (1) demonstrating the falsity of the claims; or (2) showing that the defendant lacked a reasonable basis for making the claims, *i.e.*, "substantiation." *See, e.g.,* *FTC v. Sabal*, 32 F. Supp. 2d 1004, 1007 (N.D. Ill. 1998); *FTC v. US Sales Corp.*, 785 F. Supp. 737, 748 (N.D. Ill. 1992).

As described in Section III.A.1 above, Defendants' Web sites and email messages are replete with express representations that promise consumers amazing physical and cognitive affects. Expert analyses by medical doctors demonstrate that there is no scientific basis for the claims, and the products have no discernable effect on users. Thus, Defendants' representations are both false and unsubstantiated. Defendants' deception is not only likely to mislead consumers, but undoubtedly has caused (and continues to cause) significant monetary loss to consumers. Consumers simply would not spend \$89.90 on Defendants' products if they knew that the products did not work as claimed. Thus, Defendants have violated the FTC Act, and a temporary restraining order against Defendants' misleading advertising is warranted.

2. Defendants initiate e-mail messages that violate CAN-SPAM

Defendants' violations of the CAN-SPAM Act, 15 U.S.C. § 7701 *et seq*, the federal law regulating commercial email messages, are well-documented and widespread. Defendants are directly responsible for compliance with the law, and therefore they are liable for the systematic violations of it.⁸

⁸ A violation of CAN-SPAM is a violation of Section 5 of the FTC Act. Pursuant to Section 7(a) of CAN-SPAM, the 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))." A violation of a rule proscribed pursuant to 15 U.S.C. § 57a(a)(1)(B) constitutes 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).

a. Defendants are “initiators” of commercial email

Defendants are legally responsible for the email messages promoting their products. CAN-SPAM imposes liability for a commercial email message upon “initiators” of the messages. 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. § 7709(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. § 702(12). *See also FTC v. Phoenix Avatar*, 2004 WL 1746698, at *13 (“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 email messages at issue. The email messages market Defendants’ products and include hyperlinks in the text of the messages that direct consumers to Web sites from which Defendants directly profit. As discussed above in Section III, *supra* at p. 3, McDaid purchased the Web site addresses used in the spam messages. 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”).

b. Defendants’ commercial email messages violate CAN-SPAM

The evidence overwhelmingly shows that Defendants’ commercial email messages violate CAN-SPAM. The messages utilize false or misleading header information by being routed through forms contained on innocent third parties’ Web sites. The messages also repeatedly mislead recipients as to the nature of the email through deceptive subject headings, fail to include the opportunity to decline future email messages, and fail to include the sender’s postal address.

i. *False or misleading header information*

Defendants initiate commercial email messages that contain “header information that is materially false or materially misleading” in violation of CAN-SPAM. 15 U.S.C. § 7704(a)(1).⁹ As described above, in §III.B.1, Defendants’ messages are routed through forms contained on innocent third parties’ Internet Web sites, falsifying the routing information. This practice impairs the ability of 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.

ii. *Deceptive subject headings*

Defendants initiate commercial email 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 §III.B.2, subject headings of Defendants’ spam like “Presagia Newsletter Subscription Request,” “Re: hello,” “Wineroom Contact Form,” and “A comment from your personal blog” deceptively suggest a prior relationship with the recipient.

iii. *Failure to include opportunity to decline further email messages*

Defendants initiate commercial email messages that fail to include a “clear and conspicuous” notice of the opportunity . . . 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 §III.B.3, Defendants violate this provision by initiating messages that do not contain *any* mechanism at all to decline future email messages.

⁹ 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” including “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).

iv. *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 email message demonstrates that Defendants fail to include a valid postal address in violation of CAN-SPAM. (*See* PX 11, Att. B.)

C. The Balance of the Equities Favors the FTC

The FTC respectfully requests that this Court enter a narrowly tailored TRO that brings 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 "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 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.

1. The FTC seeks a narrowly-tailored TRO

The FTC requests that the Court issue a TRO that prospectively prohibits law violations and preserves assets and documents to ensure that the Court can grant effective final relief at the conclusion of this case. Sections I-IV of the Proposed TRO contain conduct prohibitions to ensure further compliance with the FTC Act and CAN-SPAM. Sections V-IX contain asset preservation and accounting provisions aimed at identifying and preserving funds obtained unlawfully by Defendants, and identifying individuals or entities who have acted in concert or participation with Defendants. The remainder of the Proposed TRO contains reporting and discovery provisions to obtain information relevant to a preliminary injunction hearing. These are necessary provisions to identify the scope of the unlawful practices, other participants, and the location of ill-gotten gains. Defendants have no legitimate right to continue unlawful conduct, dissipate their unlawful profits or conceal information needed to effectuate relief in this case.¹⁰

¹⁰ The TRO provisions, including the asset preservation provisions, should apply to the

2. The TRO would work no valid hardship on Defendants

The balance of equities tips strongly in the FTC's favor. The FTC's proposed TRO would prohibit Defendants from making false claims about products, would stop Defendants and their agents from sending commercial email messages that violate CAN-SPAM, and would preserve assets for equitable monetary relief. 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. *See, e.g., FTC v. World Wide Factors*, 882 F.2d 344, 347 (9th Cir. 1989) (upholding finding of "no oppressive hardship to defendants in requiring them to comply with the FTC Act, refrain from fraudulent representation or preserve their assets from dissipation or concealment").

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).

3. Ex parte relief is necessary

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 may be heard in opposition. *See* Fed. R. Civ. P. 65(b). Here, as in similar FTC actions in this district where courts have granted an *ex parte* TRO,¹¹ there is a tangible risk that assets from the illegal activity, as well as relevant

individual defendant, Brian McDaid, as well as Sili. 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 should have had knowledge of the deceptive practices of the business. *See Bay Area*, 423 F.3d at 636. Here, as explained above in Section III, McDaid has intimate knowledge and extensive participation in the business affairs. He is the sole officer of Sili. He applied for Sili's merchant account to accept credit cards on the Web sites, he purchased Internet services for Sili to conduct business, and he is the sole signatory of Sili's bank account.

¹¹ Courts in this district have recently granted *ex parte* TROs under similar circumstances. *FTC v. Cleverlink Trading Limited*, 05 C 2889 (N.D. Ill. May 15, 2005) (St. Eve., J.) (granting *ex parte* TRO and asset freeze for violations of CAN-SPAM Act); *FTC v. Harry*, 04 C 4790 (N.D. Ill. July 27, 2004) (Manning, J.) (granting *ex parte* TRO and asset freeze for violations of FTC Act and CAN-SPAM); *FTC v. Phoenix Avatar LLC*, No. 04 C 2897 (N.D. Ill. April 23, 2004) (Holderman, J.) (granting *ex parte* TRO and 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 and asset freeze for violations of

documents, will disappear if Defendants receive prior notice. As described in Section III above, Defendants already have demonstrated their ability to hide their identities. They use false addresses and routing information in their email messages. They provide false registration information for Internet domain names that they purchase to market their products. They identify themselves to consumers as a company in the Caribbean.


In addition, Defendants regularly transfer funds overseas and to digital currencies. Since December 2005, over \$168,000 deposited into the Sili account has been transferred to bank accounts in a dozen foreign countries, including Switzerland, Estonia, Latvia and Russia. (PX 1 ¶¶ 28-29; PX 9.) Moreover, since May 2006, over \$100,000 has been transferred into a digital currency registered as a corporate entity in the Republic of Panama. (PX 1 ¶ 29.) In sum, *ex parte* relief is necessary to preserve the status quo and ensure that Defendants cannot move assets and records outside of this Court's reach.

V. CONCLUSION

Defendants have caused and are likely to continue to cause consumer injury because of FTC Act and CAN-SPAM 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
Marissa J. Reich
Federal Trade Commission
55 W. Monroe St., Ste. 1825
Chicago, IL 60603
Voice: (312) 960-5634
Facsimile: (312) 960-5600

FTC Act concerning commercial email marketing work-at-home scheme); *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 email marketing deceptive sale of domain names).

ATTACHMENT A

Only the Westlaw citation is currently available.

United States District Court,
N.D. Illinois, Eastern Division.

FEDERAL TRADE COMMISSION, Plaintiff,
v.
PHOENIX AVATAR, LLC d/b/a Avatar Nutrition;
DJL, LLC; Daniel J. Lin; Mark M.
Sadek; James Lin; and Christopher M. Chung d/b/a
Ait Herbal Marketing
Defendants.

No. 04 C 2897.

July 30, 2004.

Steven M. Wernikoff, William Joseph Hodor, Jason K.
Bowler, Federal Trade Commission, Chicago, IL, for
Plaintiff.

Juan A. Mateo, Law Offices of Juan A. Mateo, John
M. McManus, McManus Law, PLLC, Gerald K.
Evelyn, Law Offices of Gerald K. Evelyn, Coral M.
Watt, Attorney at Law, Detroit, MI, Evan A. Hughes,
Law Offices of Evan A. Hughes, Chicago, IL, for
Defendants.

*MEMORANDUM OPINION AND ORDER
GRANTING PRELIMINARY INJUNCTION*

HOLDERMAN, J.

*1 Before this court is the Federal Trade Commission's ("FTC") request for a preliminary injunction to be entered against defendants Daniel J. Lin, Mark M. Sadek, James Lin, and Christopher Chung. A Temporary Restraining Order ("TRO") against these defendants was entered on April 23, 2004 (Dkt. No. 6) and has continued by consent pending this ruling. Defendants Phoenix Avatar, LLC and DJL, LLC have failed to appear and a preliminary injunction was entered against these defendants on May 6, 2004. (Dkt. No. 14.) The request for a preliminary injunction against remaining defendants Daniel Lin, Mark Sadek, James Lin, and Christopher Chung is based on

purported violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), 15 U.S.C. § 7701 et seq. and 15 U.S.C. §§ 45(a), 52(a) ("FTC Act"). For the following reasons, the request for a preliminary injunction is granted.

JURISDICTION AND VENUE

This court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 1337(a) & 1345. The defendants have made a request that this action be transferred to the United States District Court for the Eastern District of Michigan for further proceedings, or, in the alternative, for this court to stay these proceedings. Neither of these requests are supported with any argument or law and are denied. Venue is appropriate in the Northern District of Illinois because defendants have transacted business here, [FN1] see 15 U.S.C. § 53(b), and defendants have provided no sufficient reason why these proceedings should be stayed.

[FN1]. See (PX 1, ¶¶ 13-28); (PX 1 ¶ 23, Att. J at 5); (PX 1 ¶¶ 32- 33); (PX 1, ¶ 35(d)).

FINDINGS OF FACT

Based on the evidence presented in the record, the court makes the following factual findings.

I. Background; FTC's Preliminary Investigation Which Led to Avatar

Theresa J. Bresnahan ("Bresnahan"), paralegal specialist with the FTC, presented most of the FTC's evidence in support of a preliminary injunction. Bresnahan testified that an e-mail consists of two parts, a header and a body. [FN2] (PX 1.) Among other things, the header usually contains identifying information fields such as the intended recipient, the sender of the e-mail, the date, and a subject line. Oftentimes, the e-mail body will contain a hyperlink, which is a link to a specific Web site on the Internet. When a user "clicks" on a hyperlink, that user's Internet browser opens up on the specified Web site. A domain name, which is usually purchased by a user, is a unique name that identifies a Web site. For example,

www.xyz.com. A sub-page designation identifies subsequent Web pages within the main Web site. For example, "info" is the sub-page designation in *www.xyz.com/info*, and clicking on this as a hyperlink would take the user to the "info" sub-page within the *www.xyz.com* Web site.

FN2. Bresnahan submitted declarations. At the hearing, Bresnahan briefly testified on direct, affirming these previous declarations. For convenience, the court refers to statements in Bresnahan's declarations as testimony.

According to Bresnahan, Internet promoters will often use an "affiliate system" to promote their products or services. Promoters recruit affiliates to assist in advertising, oftentimes resulting in affiliates sending out e-mails advertising the promoter's product. Affiliates are ordinarily paid on a commission basis and are assigned a unique identifier or "affiliate moniker." This affiliate moniker is usually appended to the end of a hyperlink contained in an e-mail advertising the promoter's product. The affiliate moniker allows the promoter to track the affiliate's success, and allows the affiliate to obtain commissions. For example, in the hyperlink *www.xyz.com/info?id=123*, "123" is the affiliate moniker. The promoter is able to track sales generated by this hyperlink to the person assigned the particular affiliate moniker "123."

*2 Bresnahan testified that the FTC maintains, for law enforcement purposes, an e-mail address where consumers can forward unsolicited commercial e-mail messages, commonly referred to as "spam." These e-mails are stored in a searchable database ("spam database"). As part of her duties as a paralegal specialist with the FTC, Bresnahan was asked to search the FTC's spam database as well as commercial Internet newsgroups for suspected misleading or deceptive spam. After reviewing a number of spam messages containing a variety of domain names, Bresnahan began to recognize two similarities among certain hyperlinks. First, she noticed that the structure of certain hyperlinks was similar in that these hyperlinks shared similar sub-page designations ending in similar affiliate monikers. For example, Bresnahan testified that a typical hyperlink in the spam she reviewed was formatted as follows:
"www.keeptoyourmatehappy.biz/m2/index.php?affid=m4," or
"www.countupandlookaway.com/m2/index.php?aff

id=m4." Second, Bresnahan began to notice that hyperlinks with these similar sub-page designations were linked to Web sites selling certain products. For example, hyperlinks containing the sub-page designation "m2" were linked to Web sites selling the Med Diet Patch, a purported weight-loss product.

Finally, Bresnahan began to notice that the hyperlinks described above, containing similar sub-page designations and affiliate monikers, frequently linked to Web sites with similar looking content. The hyperlinks with similar sub-page designations and affiliate monikers led to Web sites with similar content even though the domain names were often different. This led Bresnahan to draw the inference that this certain variety of domain names she encountered were all related to the same enterprise. As a result of this inference, Bresnahan and others at the FTC began to compile a list of all these domain names they believed to be related. The FTC designated these related domain names the "Avatar" domain names. According to Bresnahan, the FTC identified 108 Avatar domain names. (PX 1, Att. A.)

In the course of this investigation, FTC personnel visited the Web sites of domain name registrars to obtain information on who had registered the various Avatar domain names. The 103 Avatar domain names for which domain name registration information was available are purportedly registered to twenty-two persons or entities located in various countries throughout the world, including: South Africa, Lithuania, India, Singapore, Taiwan, Korea, France, Russia, Argentina, Malaysia, Turkey, Mexico and China. (PX 1, Att. B.)

II. Undercover Purchases

For purposes of investigating the Avatar domain names, Bresnahan posed as a consumer, using an alias and undercover information, including a shipping address, telephone line, e-mail address and a VISA credit card account. Bresnahan made four purchases from Web sites with Avatar domain names, two of which are relevant to the instant request for a preliminary injunction. Bresnahan linked to these Web sites by clicking on hyperlinks contained in spam received from the spam database or commercial Internet news groups.

A. First Undercover Purchase: Med Diet Patch from countupandlookaway.com

*3 On January 9, 2004, Bresnahan used a personal computer to visit the Web site www.countupandlookaway.com/m2/index.php?AFF_ID=m4 ("countupandlookaway.com"), for the purpose of purchasing the product sold on that Web site, a Med Diet Patch. A printed copy of the countupandlookaway.com Web site was admitted into evidence. (PX 1, Att. C.) The home page, or initial page encountered when visiting countupandlookaway.com, included five links leading to five separate sub-pages: PRODUCT INFO, TESTIMONIALS, FAQ'S, CONTACT, ORDER NOW. Despite the sub-page entitled CONTACT, this Web site contained no information identifying the seller. There was no telephone number, address, e-mail address or other identifying information. The CONTACT sub-page purportedly allowed a consumer to contact the seller by submitting an online form. (PX 1, Att. C, p. 6.)

To purchase the Med Diet Patch, Bresnahan clicked on the hyperlink "ORDER NOW" which took her Internet browser to the sub-page used to place orders ("Order Page"). (PX 1, Att. C at 8-9.) The Order Page was entitled "Diet Patch Secure Order Form," and it required the entry of identifying and payment information. Bresnahan entered the corresponding undercover information and clicked on a button marked "Click to Authorize" to complete the \$59.95 purchase for the Med Diet Patch. [FN3] After submitting the order, Bresnahan's Internet browser was directed to a confirmation page. This page stated that the charge appearing on the FTC's undercover credit card would appear as "AIT" or "MYPAYSYSTEMS." (PX 1, Att. C at 10.)

FN3. The completed Order Page was admitted into evidence with the undercover FTC information redacted. See (PX 1, Att. C at 8-9.)

MyPaySystems is a credit card processor located in Quebec, Canada, which maintains its own Web site: www.mypaysystems.com. This Web site allows consumers to inquire about credit card charges processed by MyPaySystems. Upon entering the credit card information used to make a purchase processed through MyPaySystems, a consumer can access an "Order Details" page produced by MyPaySystems. With respect to Bresnahan's purchase of the Med Diet Patch, on January 14, 2004, MyPaySystems listed the Vendor Company Name as "PHOENIX AVATAR,

LLC," the Vendor's Customer Support Line as (866) 248-1101, and the Vendor's Web site as www.avatarnutrition.com. See (PX 1, Att. D.)

On or about January 14, 2004, a package was received in response to Bresnahan's undercover purchase of the Med Diet Patch. The package was addressed to the undercover alias used by Bresnahan and it was marked as having been sent by Avatar Nutrition at P.O. Box 251570, West Bloomfield, Michigan. See (PX 1, Att. F.) Contained in the package was an invoice dated January 9, 2004, from "AIT Herbal Marketing/Avatar Nutrition." (PX 1, Att. H.) The telephone number appearing on the invoice--(866) 248-1101--was the same telephone number appearing on the MyPaySystems's Order Details page. The invoice also listed an e-mail address at support@aitmarketing.com and a Web site address at www.avatarnutrition.com. A printed copy of www.avatarnutrition.com was entered into evidence. (PX 1, Att. I.) The package contained a product called "Premium Diet Patch." (PX 1, Att. G.)

B. Second Undercover Purchase: Slim Form Patch from keepyourmatehappy.biz

*4 On February 24, 2004, Bresnahan purchased a product entitled Slim Form Patch from www.keepyourmatehappy.biz/m2/index.php?AFF_ID=4 ("keepyourmatehappy.biz"). (PX 1, Att. J at 1-9.) This Web site was similar to the countupandlookaway.com Web site in that it contained no information identifying the seller. In a manner similar to the first undercover purchase, Bresnahan submitted a \$59.95 order for a Slim Form Patch, and just as with the first purchase, her Internet browser was directed to a confirmation page that informed her the charge appearing on her credit card statement would appear as "AIT." (PX 1 at 12.)

In response to this purchase, the FTC's undercover credit card account was billed the \$59.95 by AIT Herbal Marketing. (PX 4, Att. A.) The FTC offered evidence that this credit card charge was facilitated by a credit card processor called First Data. See (PX 5.) Records from First Data show defendant Daniel Lin, as the purported owner of AIT Herbal Marketing, opened a merchant account with First Data. (PX 5, FDC003.) These records also show the actual FTC credit card charge for this second undercover purchase in a log compiled by First Data for AIT Herbal Marketing charges. (PX 5, FDC00386.)

On or about February 26, 2004, a package was

received at the undercover address in response to the purchase of the Slim Form Patch. The box was addressed to the alias used by Bresnahan and sent via FedEx delivery. There was no invoice in the box. However, the FedEx label was marked as having been sent by Avatar Nutrition from P.O. Box 251570, West Bloomfield, Michigan. (PX 1, Att. K.) This address and the name Avatar Nutrition were also listed on the invoice received from the first undercover purchase. The product contained in the package was a Premium Diet Patch, the same product the FTC received in response to its first purchase. (PX 1, Att. L.)

III. Representations on the Web Sites and Product Packaging

The Web site countupandlookaway.com contained various representations about the Med Diet Patch. A banner is sprawled across the top of the home page and sub-pages in a font larger than most of the other text on the pages. The banner contains the term "Med DIET PATCH," with three purported attributes listed directly under the term in similarly large font: "BURNS FAT", "INCREASES ENERGY", "CONTROLS APPETITE". (PX 1, Att. C., p. 1.) Also present in large font near the top of the home page are the following phrases: "LOSE WEIGHT THE EASY WAY," "IT'S NOT A DIET ... IT'S A PATCH." (*Id.*) The body of the text on the home page begins with, "Med Diet Patch is a cutting-edge, advanced appetite suppressant, metabolism booster, and energy enhancer ... all in one!" and also contains the sentence, "Just place a new adhesive skin patch anywhere on your body, each day for continuous, safe, and effective weight loss." (*Id.*)

This Web site keepyourmatchappy.biz contained this representation: "About The Patch: Slim Form Patch is a highly effective weight loss patch developed in Europe by Danish scientists and French biologists ." (PX 1, Att. J at 1.) The same page contained the representation: "Non-invasive safe and easy to use, this patch guarantees weight loss with dramatic results." (*Id.*) The Web site also stated: "Slim For Patch is a 'steady' weight loss system. This means you lose fat. While the patch is working to turn fat into toned muscle, you can eat normally ..., without dieting." (*Id.* at 3.)

*5 The FTC received a Premium Diet Patch in both of its purchases. (PX 1, Att G, Att. L.) On the front of the packaging of this product, directly under the name Premium Diet Patch, is the phrase "WEIGHT LOSS FORMULA." The back of the package states the

following:

The Premium Diet Patch is specifically formulated to safely stimulate your metabolism, causing your body to use and absorb food more efficiently and to burn fat rather than store it. The patch will assist in decreasing your appetite as well as increasing your energy, helping your body to lose weight naturally. Use the Premium Diet Patch every day until you reach your desired weight. It's safe, natural, and easy to use!

(*Id.*) The back of the package also contains a set of directions, a list of ingredients, and the following disclaimer: "These statements have not been evaluated by the Food and Drug Administration. This product is not intended to diagnose, treat, cure or prevent any disease." (*Id.*)

IV. Paper Trail Leading to the Defendants

A. Corporate Information

The FTC introduced evidence regarding the following information. Phoenix Avatar, LLC (the name MyPaySystems listed as the vendor of the first undercover purchase) was organized in Nevada on September 30, 2003, with a registered agent listed as EastBiz.com, Inc. (PX 1, Att. M.) Records from EastBiz.com pertaining to the formation of Phoenix Avatar, LLC were also introduced into evidence. (PX 10.) These records show that defendant James Lin, with a billing address of 1350 Chapin, Birmingham, MI, 48009 paid the \$833 fee to EastBiz.com required to form an LLC in Nevada. (PX 10, EB003.) As described below, the records for bank account number 884282030 with National City Bank, controlled by defendants Daniel Lin, James Lin and Mark Sadek, show an \$833 payment to EastBiz.com. (PX 7, EB 00105 .)

The FTC introduced into evidence a filing for a Michigan Business Fictitious Name; "AIT HERBAL MARKETING," with a business address of 634 Woodward Ave., 4th F, Detroit, 48226. (PX 15.) The record listed a contact name and contact address as defendant Christopher Chung, 7080 Ten Hill Dr., West Bloomfield, MI. (PX 15.) The FTC also offered evidence showing that "Ait Herbal Mkt," with an address of 7080 Ten Hill Dr., W. Bloomfield, MI, through Mark Sadek, applied for P.O. Box 251570 in West Bloomfield Michigan (the address both undercover purchases were received from). (PX 4, Att. P.) The FTC also introduced evidence received from AT & T Corporation relating to the telephone number information it received in making the first undercover

purchase of the Med Diet Patch. This telephone number--(866) 248-1101, which was provided by MyPaySystems as the Vendor's Customer Support Line for the first undercover purchase, and listed on the invoice the FTC received in regard to the first undercover purchase--was registered to AIT Herbal Marketing, located at 7080 10 Hill Street, West Bloomfield Michigan. (PX 1, Att. P). AT & T listed the contact name on the account as defendant Mark Sadek. (*Id.*)

*6 Finally, the FTC offered evidence regarding a filing for a Michigan domestic limited liability company, DJL, LLC. (PX 1, Att. O .) Defendant Daniel Lin was listed as the agent for DJL, LLC in this filing, which listed the registered office address as 1350 Chapman, Birmingham, MI, 48009. (*Id.*)

B. Financial Records

The FTC also offered evidence regarding a bank account number 884282030 with National City Bank in the name of DJL, LLC. (PX 1, Att. Q; PX 7, NCB0095.) The signatories on this bank account are defendant Daniel Lin, President; defendant James Lin, Vice President; and defendant Mark Sadek, Director of Operations. Examination of the records of this bank account showed frequent deposits from various credit card merchant processors. (PX 7, NCB0095, NCB 00107-110.) According to Bresnahan, examination of the bank records indicates that from September 2003 to January 2003 the total amount deposited into this bank account was approximately \$462,600. (PX 1 ¶ 34(c).) The records also indicate that a payment of \$833 was made to EastBiz.com. (PX 7, EB 00105).

The FTC also introduced evidence regarding an account with the credit card processor First Data. (PX 5.) Defendant Daniel Lin opened a merchant account with First Data under the name AIT Herbal Marketing. (PX 5, FDC003.) The AIT Herbal Marketing merchant account with First Data was identified as account number 267765788885. (PX 5, FDC00386.) The AIT Herbal Marketing merchant application with First Data instructed that credit card payments be deposited into bank account number 884282030. (PX 5, FDC003.) The records of bank account number 884282030 identify repeated deposits from "MERCHANT BANKCD 26776578885" from September 2003 through March 2003. (PX 7, NCB 0097-98, 107-110, 132-33.)

The FTC also offered evidence showing that the

defendants purchased numerous Premium Diet Patches from a company called EyeFive in California. Defendant James Lin first contacted EyeFive in late August of 2003 to make a wholesale inquiry that led to the purchase of 500 bottles of VP-RX virility pills. See (PX 12, EF00505-06.) In early November 2003, EyeFive informed Defendant James Lin that it was now marketing the Premium Diet Patch. (PX 12, EF00389-91.) In mid-November 2003, Lin bought 500 premium diet patches for \$5.67 each. (PX 12, EF00402; EF0023.) He bought another 200 diet patches in March of 2004, (PX 12, EF0035), and he ordered another 100 diet patches on April 27, 2004. (PX 12, EF0047; EF0027.) All of these products were shipped to DJL, LLC, with an address in New York, New York. (PX 12, EF0023; EF0035; EF0047.)

V. Expert Testimony Regard the Efficacy of the Premium Diet Patch

The FTC presented evidence from Michael Jensen M.D. ("Jensen"). Jensen is a professor of medicine at the Mayo Medical School, located in Rochester, Minnesota, and a member of the Endocrine Research Unit of the Mayo Clinic. (PX 2 ¶ 1.) Jensen reviewed printouts of the two Web sites, countupandlookaway.com and keepyourmatchhappy.biz, as well as a photocopy of the Premium Diet Patch. Jensen found, based upon his professional experience and knowledge, "that none of the ingredients listed on the weight-loss patch label and web site, separately or together, could cause any weight-loss." (*Id.* ¶ 9.) Jensen also found that "none of the ingredients listed on the weight loss patch label and web site, separately or together, could cause an increase in metabolism, a decrease in appetite, and a reduction of food cravings, thereby enabling users to lose substantial, or any weight." (*Id.* ¶ 10 .)

*7 Under cross-examination Jensen stated that "the standard scientific approach to testing a patch product would be to give an active patch to a group of people and a placebo patch to a group of people and determine the effects between the two groups." (June 4, 2004 Hrg. Tr. at 44.) Jensen did not perform this type of scientific testing and testified that such testing would not have been helpful because the ingredients listed on the Web sites and on the Premium Diet Patch packaging had not been found "individually or in combination in the literature to provide a reasonable mechanism of action that could allow one to predict that they would have the effects they were claimed to have." (*Id.*)

The defendants introduced into evidence an excerpt from a television broadcast. (DX H.) In this excerpt, a television news show identified as channel 4, but with no city or geographic location noted, compared the effects of four common weight loss products: Slim Fast, a diet patch, diet and exercise, and surgical intervention. (June 4 2004 Hrg. Tr. at 69.) Four contestants were each asked to utilize one of the respective diet methods over a period of four weeks, and the result was that a Mr. Ortiz, who utilized a diet patch, claimed to have lost 25 pounds over a four week period. (*Id.*) In response to this evidence, Dr. Jensen testified that (1) four weeks is not an adequate time test for treatments of obesity, the Food and Drug Administration, for example, requires one to two years of testing to approve a new product for obesity treatment (June 4 2004 Hrg. Tr. at 66); (2) Mr. Ortiz's claimed success with a diet patch was not probative because Mr. Ortiz was biased as to the outcome of using the patch (*Id.* at 69); and (3) that this test was at most anecdotal evidence. [FN4]

FN4. The defendants also introduced a number of documents relating to the efficacy of certain herbal supplements in weight loss. Defendants have chosen not to rely upon any of these exhibits in their closing argument, and the court, accordingly, will not consider these documents.

VI. Expert Testimony Regarding Spam

The defendants called Paul H. Howell ("Howell"), Chief Information Technology Security Officer at the University of Michigan, Ann Arbor, Michigan to testify. *See* (Defs.' Ex. V; Dkt. No. 39, Att. N.) In his "Preliminary Report," Howell explained that e-mail sender and receiver information can be easily forged. (Defs.' Ex. W at 1; Dkt. No. 39, Att. M at 1.) To explain how this information is forged, Howell analogized e-mail to regular mail (e.g., United States Postal Service). (*Id.* at 2.) Howell explained that both types of mail utilize an outer envelope. The senders of both types of mail generally place their return address on the outer envelope. However, with both types of mail it is possible to provide misleading information in the form of a false return address, which is unreliable for determining the source of the mail. Both types of mail also contain postmarks: computers, which process and forward e-mail, insert a line of text that is analogous to a postmark stamp in regular mail. This "electronic

postmark" includes date and time stamps that can be used to trace back the origin of an e-mail. It is possible, however, to insert misleading electronic postmarks in an attempt to conceal the source of an e-mail. Howell testified that the sender information on the e-mails introduced into evidence by the FTC had been forged in an attempt to thwart the identification of the true sender.

*8 According to Howell, the only reliable method for tracing an e-mail back to its true origin is to confirm the validity of the electronic postmarks and follow those back to the original sending computer. Once the originating computer has been identified, various means may be used to determine who actually sent the e-mail. Howell testified that the FTC failed to follow this procedure by not attempting to identify the sending computer of the e-mails by tracking back the information in the electronic postmarks. Howell concluded that there is no circumstantial or direct technical evidence that links the sending of the e-mails in this case to any particular person. Howell also concluded that the sender information on the e-mails introduced into evidence by the FTC had been forged in an attempt to thwart the identification of the true sender.

The FTC introduced an expert report from Brent Dylan-Rudy Deterding ("Deterding"), Senior Security Analyst at LURHQ, a managed security services provided in Chicago, Illinois. (PX 25.) Deterding testified that senders of spam ("spammers") go to great lengths to obfuscate the true and complete transmission path spam takes.

Deterding testified that spammers' preferred method for hiding their identity is to utilize an "open proxy." (*Id.*) An open proxy is a computer that, with or often without the owner's knowledge, accepts connections from anyone, anywhere, and forwards the e-mails from those connections as if the e-mails had originated from the open proxy. According to Deterding, these open proxies result from either (1) insecure software that allows a spammer to utilize the open proxy or (2) software maliciously installed on a computer, such as worms, Trojan horses or viruses that turn the computer into an open proxy. (*Id.* at 2.) Deterding's report stated that it is a widely held opinion in the computer industry that a majority of spam is sent using open proxies. (*Id.*) Furthermore, ComCast, the nation's largest Internet Service Provider, estimates that nearly 90% of e-mail sent on its network is spam sent through open proxies. (*Id.*) (citation omitted). Deterding testified that the use of open proxies makes tracing e-mail back to its true source near impossible. (*Id.* at 3.) Finally, Deterding

concluded that the e-mails introduced by the FTC, that led to the two Web sites countupandlookaway.com and keepyourmatchappy.biz, were sent through open proxies, and, therefore, that there is not a reliable, accurate, technical method to determine the sender of these spam messages. (*Id.* at 4.)

STANDARD OF REVIEW

This court reviews the FTC's request for an injunction pursuant to 15 U.S.C. § 53(b) under the "public interest" test, which requires that this court to (1) determine the FTC's likelihood of success on the merits, and (2) balance the equities. *FTC v. Word Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1028-29 (7th Cir.1988) ("We believe that the legislative history of section 13(b) makes it quite clear that the 'public interest' test is the correct approach."). Under the "public interest" test, "the FTC need not prove irreparable injury to obtain a preliminary injunction." *Kinney v. Int'l Union of Operating Eng'rs, Local 150, AFL-CIO*, 994 F.2d 1271, 1277 (7th Cir.1993). The threshold showing of a likelihood to succeed under the traditional test is a better than negligible chance of success on the merits, and this court adopts that standard here. See *Cooper v. Salazar*, 196 F.3d 809, 813 (7th Cir.1999).

*9 Under the public interest test, "private concerns may certainly be considered, [but] public equities must receive far greater weight." *World Travel Vacation Brokers, Inc.*, 861 F.2d at 1029; see also *FTC v. Weyerhaeuser Co.*, 665 F.2d 1072, 1083 (D.C.Cir.1981) ("When the Commission demonstrates a likelihood of ultimate success, a countershooting of private equities alone would not suffice to justify denial of a preliminary injunction."). That is not to say, however, that private equities receive no weight, as the Seventh Circuit has explained: "While not giving controlling weight to 'private equities'--of course not--the cases give them some weight." *FTC v. Elders Grain, Inc.*, 868 F.2d 901, 903 (7th Cir.1989). "[P]rivate equities are entitled to serious consideration," especially where the defendant "can show irreparable injury to it from the grant of an injunction." *Id.* "[I]f the defendant can show irreparable injury to it from the grant of the injunction, then merits and harms must be evaluated in the usual way." *Id.* This "usual way" would involve a "sliding scale" approach. *Id.*; see also *Tv, Inc. v. Jones Group Inc.*, 237 F.3d 891, 895-96 (7th Cir.2001). This sliding scale approach requires that the court factor the FTC's probability of success on the merits into the balance of the harms. Thus, "[t]he

greater the plaintiff's likelihood of success on the merits ... the less harm from denial of the preliminary injunction the plaintiff need show in relation to the harm that the defendant will suffer if the preliminary injunction is granted." *Elders Grain, Inc.*, 868 F.2d at 903. "The sliding scale approach is not mathematical in nature, rather 'it is more properly characterized as subjective and intuitive, one which permits district courts to weigh the competing considerations and mold appropriate relief.'" *Tv, Inc.*, 237 F.3d at 896 (citations omitted).

ANALYSIS

I. FTC's Likelihood of Success on the Merits

To establish a likelihood of success on the merits, the FTC must show a violation of the law that the defendants committed. The two statutes allegedly violated by the defendants are the FTC Act and CAN-SPAM. The court will first address whether these statutes have been violated and then, evaluating all of the evidence, the court will analyze the FTC's likelihood of success in establishing the defendants' liability at a trial on the merits.

A. Violations of the FTC Act and CAN-SPAM

(i) FTC Act

The FTC Act states, in pertinent part: "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful." 15 U.S.C. § 45(a)(1). The FTC Act also prohibits the dissemination of false advertisement for the purpose of inducing the purchase of a drug or device. 15 U.S.C. § 52(a). The FTC Act deems such dissemination of false advertisement "an unfair or deceptive act of practice in or affecting commerce within the meaning of section 45." 15 U.S.C. § 52(b). The Seventh Circuit has explained that "representations ... likely [to] mislead consumers, acting reasonably, to their detriment" are deceptive within the meaning of section 45(a)(1) of the FTC Act. *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1029 (7th Cir.1988) (citation omitted). "In addition, '[m]isrepresentations of material facts made for the purpose of inducing consumers to purchase services constitute unfair or deceptive acts or practices." *Id.* (citation omitted). The "misrepresentation or practice need not be made with an intent to deceive" to violate the FTC Act. In general, advertisements are considered deceptive if the proponent lacked a reasonable basis for asserting its

truth. See *Kraft, Inc. v. FTC*, 970 F.2d 311, 314 (7th Cir.1992); *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1096 (9th Cir.1994); *Thompson Medical Co. v. FTC*, 791 F.2d 189, 193-94 (D.C.Cir.1986). See also *FTC v. Sabal*, 32 F.Supp.2d 1004, 1007 (N.D.Ill.1998).

*10 This court rules that the FTC has a better than negligible chance of success on the merits of its claim that the representations regarding the Premium Diet Patch ("diet patch") are deceptive. The Web sites and packaging of the diet patch made express claims that the diet patch would cause weight loss by suppressing appetite and boosting metabolism. The packaging represented that the diet patch was a "weight loss formula," and that using the diet patch would "safely stimulate your metabolism, causing your body to use and absorb food more efficiently and to burn fat rather than store it." The two Web sites that the FTC utilized to purchase the product contained similar representations, describing the diet patch as "a highly effective weight loss patch."

The evidence presented at the hearing showed that these representations were false. In sum, Dr. Jensen testified that there is no scientific evidence relied upon by the medical community that would suggest that the diet patch the defendants sold or advertised on the two Web sites would cause any weight loss, increase metabolism, or decrease appetite. The evidence submitted by the defendants to the contrary does not detract from Dr. Jensen's conclusions, and certainly does not provide substantiation for the defendants' contention that the diet patch representations are not deceptive.

The defendants argue that the following disclaimer, present on the diet patch packaging, proves that it does not violate the FTC Act: "These statements have not been evaluated by the Food and Drug Administration. This product is not intended to diagnose, treat, cure or prevent any disease." But this disclaimer does not address, much less deny, the representations regarding weight loss and therefore cannot cure the deceptive representations. *FTC v. U.S. Sales Corp.*, 785 F.Supp. 737, 751 (N.D.Ill.1992) ("Disclaimers or qualifications in any particular ad are not adequate to avoid liability unless they are sufficiently prominent and unambiguous to change the apparent meaning of the claims and to leave an accurate impression.")

The main thrust of defendants' opposition to liability under the FTC Act is the argument, without any citation to legal authority, that the FTC cannot be successful on

the merits of its claims without providing evidence of a specific consumers being "defrauded" or harmed. The FTC has made the required showing that the defendants' claims are false, and therefore "deceptive" under the act. The FTC has also made the required showing that consumers relied upon these deceptive claims. "[O]nce the FTC shows (1) that a reasonably prudent person would rely on the deceptive advertisements, (2) that these advertisements were widely disseminated, and (3) that consumers purchased the product, [t]he burden shifts to the defendants to prove that the representations were not relied upon by the consumers." *FTC v. World Traveler Vacation Brokers, Inc.*, 861 F.2d 1020, 1029 (7th Cir.1988) (citation omitted). The false representations about weight loss were disseminated over the Internet and the FTC has presented evidence establishing that the defendants purchased at least 800 diet patches in three separate orders over a six-month period. The fact that defendants continued to purchase diet patches leads to the conclusion that consumers were purchasing the diet patches—a conclusion buttressed by the bank records indicating numerous deposits into the defendants' bank account from credit card processors.

*11 Accordingly, this court rules that the FTC has demonstrated a better than negligible chance of success on the merits of its claims that representations on the Web sites *countupandlookaway.com* and *keepyourmatchappy.biz*, as well as on the packaging of the diet patch violate the FTC Act.

(ii) *Violations of CAN-SPAM*

On January 1, 2004, the Controlling the Assault of Non-solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") went into effect. In this legislation, Congress made the finding that electronic mail had not only "become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis," but that it also served an important role "for the development of frictionless commerce." 15 U.S.C. § 7701(a)(1). These great benefits for society and economy are, however, "threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail." § 7701(a)(2). According to Congress, unsolicited commercial electronic mail, or spam, "account[s] for over half of all electronic mail traffic, up from an estimated 7 percent in 2001." § 7701(a)(2). The prevalence of spam significantly detracts from the efficiency and convenience of electronic mail. See §§ 7701(a)(3), (a)(4), (a)(5), (a)(6). Congress specifically

listed what it considered to be the evils of spam: that its source and purpose for being sent are often disguised, §§ 7701(a)(7), (a)(8); that senders of spam often do not provide its recipients with the ability "to reject (or "opt-out" of) receipt" of the spam, § 7701(a)(9); and that senders of spam are able "to gather large numbers of electronic mail address on an automated basis from Internet websites ... where users must post their addresses in order to make full use of the website or service." § 7701(a)(10).

Based upon these findings, Congress determined that:

- (1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;
- (2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and
- (3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

§ 7701(b). Finally, CAN-SPAM specifically notes that "[i]t is the sense of Congress that ... Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems." § 7703(c).

In accordance with the preceding Congressional findings, CAN-SPAM imposes certain requirements on those who "initiate the transmission of commercial electronic mail message[s]." § 7704(a)(1). [FN5] Commercial e-mail messages must not contain materially false or misleading information regarding its source or deceptive subject headings. §§ 7704(a)(1), (a)(2). Commercial e-mail messages must contain: (1) a return email address or other "opt-out" mechanism that allows a recipient to voice his or her objection to further receipt, (2) a clear identification that it is a commercial advertisement or solicitation, [FN6] (3) a clear notice of the ability to "opt-out," and (4) the sender's physical postal address. §§ 7704(a)(3), (a)(5). CAN-SPAM also makes it unlawful to send commercial e-mails to a recipient who has "opted-out." § 7704(a)(4). A violation of CAN-SPAM "shall be enforced by the [FTC] as if the violation ... were an unfair or deceptive act or practice." § 7706(a)

[FN5]. "The term 'initiate,' when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or

transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message." 15 U.S.C. § 7702(9).

[FN6]. This requirement does not apply "if the recipient has given prior affirmative consent to receipt of the message." § 7704(a)(5)(B).

*12 There is no dispute that the e-mails in question violate CAN-SPAM. These e-mails, in fact, violate most, if not all, of CAN-SPAM's major provisions. Both of the technical experts testified at the preliminary injunction hearing that the e-mail messages marketing the two Web sites *countupandlookaway.com* and *keepyourmatchhappy.biz* concealed the identify of the sender, violating section 7704(a)(1)'s requirement that e-mail messages shall not contain "header information that is materially false or materially misleading." [FN7] Furthermore, the e-mails do contain neither a conspicuous notice of the ability to "opt-out," nor the sender's physical postal address, nor a clear notice that the e-mails are commercial solicitations. All of these omissions violate CAN-SPAM. § 7704(a)(5)(A).

[FN7]. "The term '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." § 7702(8).

While defendants have not disputed that the e-mails violate CAN-SPAM, they have attempted to mount a constitutional challenge to CAN-SPAM itself. According to the defendants, CAN-SPAM "prohibits various e-mail messages which omit certain information, and accordingly, is a content-based Internet restriction, which is presumed invalid." (Defs.' Closing at 21.) Defendants support this conclusory statement with a quote from the Supreme Court's recent decision in *Ashcroft v. American Civil Liberties Union*, --- U.S. ---, 124 S.Ct. 2783, --- L.Ed.2d --- (2004), in which the Supreme Court held that the Child Online Protection Act ("COPA"), 47 U.S.C. § 231, was an

invalid content based restriction. This court will only consider the single constitutional argument raised by defendants. Defendants contention that a prohibition on e-mails omitting certain information—or a requirement of disclosures—amounts to content-based restrictions on speech is rejected because it "overlooks material differences between disclosure requirements and outright prohibitions on speech." *Zauderer v. Office of Disciplinary Counsel of the Supreme Court of Ohio*, 471 U.S. 626, 105 S.Ct. 2265, 2281, 85 L.Ed.2d 652 (1985). In short, requiring disclosure of information does not amount to a content-based restriction. *See Id.* Accordingly, defendants constitutional claim fails.

B. Defendants' Responsibility for Violations of the FTC Act and CAN-SPAM

In the Finding of Facts section, the court has laid out in detail the evidence the FTC has presented to tie the defendants to the deceptive practices and violations of CAN-SPAM. The evidence connects the defendants to the entities selling the diet patches from the two Web sites `countupandlookaway.com` and `keepyourmatehappy.biz` and also establishes that the money spent purchasing the diet patches ended up in the defendants' possession.

Phoenix Avatar, LLC was listed by MyPaySystems as the vendor selling diet patches from `countupandlookaway.com`, and AIT Herbal Marketing was listed on the invoice from this purchase, and AIT Herbal Marketing appeared on the FTC's credit card statement for the second purchase. Thus, the evidence establishes that Phoenix Avatar, LLC, and AIT Herbal Marketing were selling the diet patches marketed on the Web sites `countupandlookaway.com` and `keepyourmatehappy.biz`.

*13 The fact that these entities used these Web sites to sell their products establishes that they are likely responsible for the content of the Web sites. Similarly, the entities are likely responsible for the offending spam, which functioned as advertisements for the Web sites. The offending spam contained hyperlinks to these Web sites and also contained advertisements such as "Amazing patch makes you shed the pounds!" which directed recipients of the spam to the Web sites. (PX 4, Att. L, M.) Accordingly, it is quite likely that the entities utilizing the Web sites to sell diet patches initiated the transmission of the spam advertising the Web sites.

This conclusion is not undermined by the absence of

technical evidence tracing the spam in this case back to its source. Both experts testified to the difficulties of determining the source of spam, due to the fact that those who send spam go to great lengths to hide their identities. And both experts testified that the e-mails in this case contain misleading information inserted for the purpose of obfuscating their true source. The FTC's expert also testified that no technical method existed to determine the source of the e-mails because of the use of open proxies. Technical evidence connecting a person or an entity to spam would certainly be persuasive. However, it is not necessary to prove a violation of CAN-SPAM, as the definition of "initiate" in CAN-SPAM makes clear. Liability is not limited to those who physically cause spam to be transmitted, but also extends to those who "procure the origination" of offending spam. 15 U.S.C. § 7702(9). The technical evidence attested to by defendants' expert Howell could not establish who "procure[d] the origination" of spam. Therefore, the statute necessarily contemplates the use of nontechnical evidence to prove the source of offending spam.

Finally, the evidence connects the defendants to these two entities that are likely responsible for the deceptive practices and CAN-SPAM violations described above. Defendant James Lin, utilizing his bank account 884282030 jointly controlled with defendants Daniel Lin and Mark Sadek, paid the fee required to form Phoenix Avatar, LLC. The record also establishes that defendant Christopher Chung registered the Fictitious Business Name AIT Herbal Marketing, which was listed on the invoice the FTC received from its first undercover purchase. AIT Herbal Marketing, through M. Sadek, applied for the P.O. Box 251570, from which both undercover purchases were shipped. The FTC's undercover credit card was billed by AIT Herbal Marketing for the second undercover purchase. The evidence establishes that credits to AIT Herbal Marketing's merchant account with a credit card processor were deposited into bank account 884282030. The FTC has shown that the defendants are likely the individuals acting through the entities Phoenix Avatar, LLC and AIT Herbal Marketing.

At this stage of the litigation, the court is also not swayed by defendants mere assertion that the FTC has failed to offer evidence of the defendants' "actual knowledge and/or participation in what the FTC claims to be deceptive acts and practices." (Defs.' Closing at 18.) *See FTC v. Amy Travel Service, Inc.*, 875 F.2d 564, 573-74 (7th Cir.1989). This standard applies when determining which individuals to hold liable after

corporate liability is established. *Id.* However, AIT Herbal Marketing, the entity purporting to sell both diet patches is not a corporation. It is simply a fictitious business name, and the evidence introduced by the FTC shows that the individuals using and profiting from this name are the defendants. Finally, the FTC has shown the defendants "active involvement in [the] business affairs" of Phoenix Avatar, LLC, which is "probative of [their] knowledge" of that company's deceptive acts and practices. *Id.* at 574.

*14 Accordingly, this court finds that the FTC has a better than negligible chance of success in showing that the individual defendants are responsible for the violations of the FTC Act and CAN-SPAM.

II. *Balancing The Equities*

As this court has explained, under the "public interest" test, public interests are given far greater weight than private equities, which is not to say though that private equities should not be considered, especially where the defendant may face irreparable injury. See *FTC v. Elders Grain, Inc.*, 868 F.2d 901, 903 (7th Cir.1989). The defendants contend that the public equities in this case are low or nonexistent because the FTC has failed to produce evidence of consumers complaining of harm from the defendants practices. This court disagrees. The public has an important interest in a violation of the law. The public would be harmed by continued violations of the law. The FTC has shown a high likelihood success on its claim that the defendants have violated both the FTC Act and CAN-SPAM. Accordingly, the public interest in this case is great. *Id.* (Ripple, J. concurring) ("A strong showing by the government that a violation of law has occurred necessarily produces 'public equities' that must 'receive far greater weight' than 'private equities.'").

Furthermore, despite defendants' argument to the contrary, the FTC has shown a concrete harm to individual members of the public. The FTC has shown (1) that it is likely that the defendants are misrepresenting the effects of their product to the public and (2) that the defendants are barraging the public with spam. Both of these practices cause harm to actual individuals in the public. Those who purchase the defendants' diet patches are not receiving the product for which they paid. Those who receive defendants' spam are forced to incur the costs of needlessly expended energy and time evaluating and eventually discarding defendants' unsolicited messages falsely advertising weight loss products.

This court also rejects defendants' second primary argument attacking the existence of a public interest—that other corporations and entities are selling similar diet patches and the FTC has produced no evidence that these entities are being enjoined. Defendants, unsurprisingly, cite no case law for their proposition that the public interest in enforcing the law is low when others also violate the same law. This court declines to so hold.

As the case law makes clear, a countershooting of private equities may justify denial of a preliminary injunction only when these private equities are significant. See *Elders Grain, Inc.*, 868 F.2d at 903. Defendants have not presented any irreparable injury that would justify tipping the balance of equities in their favor.

Defendants argue that the requested injunction should not be granted because "it may directly infringe" on the defendants' Fourth, Fifth and Sixth Amendment rights. (Defs.' Closing at 19.) [FN8] The fact that something "may" happen hardly amounts to irreparable injury. Furthermore, the court does not find that any of defendants' constitutional rights will be violated by the preliminary injunction. The defendants' Fifth Amendment argument is premature. *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1031 (7th Cir.1988) ("Until the ... defendants submit the proper records to the district court, and the court refuses to lift the freeze, [defendants'] self-incrimination claim is premature."). The preliminary injunction also does not prohibit the defendants from retaining counsel, nor does it prohibit defendants from using frozen funds to pay counsel. It merely requires that defendants account for funds paid to attorneys.

[FN8. In a footnote, defendants incorporate by reference their Joint Mot. to Dissolve the Ex Parte Temporary Restraining Order and reiterate their argument that the TRO violates their Fifth and Sixth Amendment rights. (Defs.' Closing at 19, n. 6). Defendants arguments regarding the ex parte nature of the TRO are moot give this court's ruling granting the FTC's request for a preliminary injunction made after the defendants have been heard.

*15 Finally, the court rejects the defendants argument that the asset freeze in particular is an unjustified burden on them due to the fact that the FTC has not

presented any evidence of consumer harm. The FTC has signaled its intent to seek restitution in the event it is eventually successful in this matter, and this court has already found a likelihood of success on its claim that defendants have engaged in deceptive practices in relation to selling diet patches. Accordingly, restitution may well be appropriate at the conclusion of this matter and this court has a duty to ensure that such restitution will be possible. World Travel Vacation Brokers, Inc., 861 F.2d at 1031 ("[T]he district court [has] a duty to ensure that the assets of the corporate defendants were available to make restitution to the injured customers.").

Considering the equities, this court finds that the balance of equities favors the FTC because the defendants have not demonstrated any significant, much less irreparable injury to them from the FTC's requested preliminary injunction. This conclusion is strengthened when the court factors into the balance the FTC's likelihood of success. For purposes of applying the sliding scale analysis, this court finds the FTC's likelihood of success on the merits as greater than a mere better than negligible chance. The FTC has amassed a persuasive chain of evidence connecting the defendants to violations of the FTC Act and CAN-SPAM. This evidence is sufficient to support by a preponderance of the evidence the finding sought by the FTC against the defendants. This strong showing, coupled with the presumption that public equities receive far greater weight than private equities, establishes that the balance of equities favors the FTC in this case.

CONCLUSION

Accordingly, the request for a preliminary injunction against defendants Daniel J. Lin, Mark M. Sadek, James Lin, and Christopher Chung is granted. It is therefore ordered that defendants, and their agents, servants, employees, attorneys, and those persons or entities in active concert or participation with them who receive actual notice of this order by personal service, or otherwise, are hereby preliminarily enjoined from doing, or assisting others in doing, the following acts:

1. Expressly or by implication:

- (a). Representing that the Med Diet Patch, Slim Form Diet Patch, or any other diet patch, causes weight loss;
- (b). Misrepresenting that any product, or any ingredient contained in it, increases metabolism, decreases appetite, and/or reduces food cravings;
- (c). Misrepresenting that any product, or any

ingredient contained in it, is effective in the diagnosis, cure, mitigation, treatment, or prevention of any disease;

(d). Making any representation about the health benefits, performance, efficacy, or safety of any product unless, at the time of making such representation, defendants possess and rely upon competent and reliable scientific evidence that substantiates the representation;

*16 (e). Misrepresenting any other fact material to a consumer's decision to purchase any product.

2. Violating the provisions contained in sections 5 and 6 of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C. §§ 7704 and 7705 by initiating the transmission of a commercial electronic mail message that:

(a). Contains, or is accompanied by, false or misleading header information in violation of section 5(a)(1) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(1);

(b). Fails to include a clear and conspicuous notice of the opportunity to decline to receive further electronic mail messages from the sender, in violation of section 5(a)(5)(ii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(ii); and/or

(c). Fails to include a valid physical postal address of the sender in violation of section 5(a)(5)(iii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(iii).

3. (a). Selling, liquidating, assigning, transferring, converting, loaning, encumbering, pledging, concealing, dissipating, spending, withdrawing, or otherwise disposing of any funds, real or personal property, or other assets or any interest therein, wherever located, including any assets inside or outside the territorial United States, which are:

(1.) in the actual or constructive possession of any defendant;

(2.) owned or controlled by, or held, in whole or in part, for the benefit of, or subject to access by, or belonging to, any defendant; or

(3.) in the actual or constructive possession of, or owned or controlled by, or subject to access by, or belonging to, any corporation, partnership, trust or any other entity directly or indirectly owned, managed, or controlled by, or under common control with, any defendant, except as agreed to by the FTC through counsel.

(b). Opening or causing to be opened any safe deposit boxes titled in the name of any defendant, or subject to access by any defendant;

(c). Incurring charges on any credit card issued in the

name, singly or jointly of any defendant;
(d). Transferring any funds or other assets subject to this order for attorney's fees or living expenses, except from accounts or other assets identified by prior written notice to the FTC; provided that no attorney fees or living expenses, other than those set forth below and only in accordance with the procedures set forth below, shall be paid from funds or other assets subject to this order.

31, 2004.

2004 WL 1746698 (N.D.Ill.)

END OF DOCUMENT

*PAYMENTS OF LIVING EXPENSES AND
ATTORNEY FEES ALLOWED*

Notwithstanding the above, any defendant may pay from his personal funds reasonable, usual, ordinary, and necessary living expenses and attorney fees. No such expenses, however, shall be paid from funds subject to this order except from an account designated by written notice to counsel for the FTC prior to the payment.

FUNDS, PROPERTY AND ASSETS AFFECTED

The funds, property and assets affected by this order shall include both existing assets and assets acquired after the effective date of this order, during the pendency of this lawsuit, including without limitation, those acquired by loan or gift, defendants shall hold all assets, including without limitation, payments, loans, and gifts, received after service of this order.

MAINTAINING RECORDS

*17 Defendants and their agents, servants, employees, attorneys, and those persons or entities in active concert or participation with them who receive actual notice of this order by personal service, or otherwise, are hereby also ordered to maintain all records in their possession or control pertaining to the above.

DURATION AND EFFECT OF THIS ORDER

This order supercedes the TRO (Dkt. No. 6) entered in this case. This order shall remain in effect during the pendency of this case, through a trial on the merits, and until entry of a final judgment or further order of court, whichever occurs first. No security is required pursuant to Federal Rule of Civil Procedure 65(d).

Counsel are to confer pursuant to Federal Rule of Civil Procedure 26(f) and file a jointly completed Form 35 Report of Parties' Planning Meeting on or before August 17, 2004. This case is set for a report on status and entry of a scheduling order at 9:00 a.m. on August