

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

FEDERAL TRADE COMMISSION,	)	
	)	
Plaintiff,	)	
	)	Case No. 07 C 4541
v.	)	
	)	Judge David H. Coar
SILI NEURACEUTICALS, LLC, and	)	
	)	Magistrate Judge Morton Denlow
BRIAN MCDAID, individually and doing	)	
business as KAYCON LTD,	)	
	)	
Defendants.	)	

**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.)<sup>1</sup> 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.)

---

<sup>1</sup> 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.)<sup>2</sup>

### 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:

HV”G”H [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.)<sup>3</sup> 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.)<sup>4</sup> 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).<sup>5</sup> 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

---

<sup>4</sup> 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.*)

<sup>5</sup> 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.)<sup>6</sup>

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.<sup>7</sup>

##### A. Injunctive Relief Standard

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

##### 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.

---

<sup>7</sup> *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.<sup>8</sup>

---

<sup>8</sup> 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).<sup>9</sup> 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.<sup>10</sup>

---

<sup>10</sup> 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,<sup>11</sup> 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. Stuffingsforcash.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.

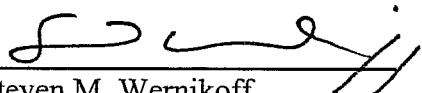
In addition, Defendants regularly transfer funds overseas and to digital currencies. Since December 2005, over \$168,000 deposited into the Sili account has been transferred to bank accounts in a dozen foreign countries, including Switzerland, Estonia, Latvia and Russia. (PX 1 ¶¶ 28-29; PX 9.) Moreover, 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).