

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

FEDERAL TRADE COMMISSION,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	Case No. 08CV5666
LANCE THOMAS ATKINSON,	)	
	)	Judge Virginia Kendall
INET VENTURES PTY LTD, an Australian proprietary company,	)	
	)	Magistrate Judge Maria Valdez
JODY MICHAEL SMITH,	)	
	)	
TANGO PAY INC., a Delaware corporation,	)	
	)	
CLICK FUSION INC., a Delaware corporation,	)	
	)	
TWOBUCKS TRADING LIMITED, a Cyprus limited liability company,	)	
	)	
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

The FTC asks the Court to take immediate action to shut down an international “spam” enterprise that deceptively markets and sells bogus “male enhancement” pills and “generic” prescription drugs that are falsely claimed to be FDA-approved. Defendants’ ongoing deceptive product sales are defrauding consumers out of millions of dollars, and the network of “spammers” that they pay to promote their products is causing considerable additional harm. Despite taking great efforts to avoid detection, the evidence shows that Australia-based Lance Atkinson and U.S.-based Jody Smith control, and profit from, this operation.

This enterprise -- which operates on the Internet under the name “Affking” -- is responsible for likely billions of illegal commercial e-mail messages and is one of the largest spam organizations in the world. The FTC has received over three million complaints regarding spam messages connected to this operation. The spam messages sent on behalf of the operation falsify information that would identify the true sender in violation of the federal CAN-SPAM law regulating e-mail marketing. The messages also illegally fail to offer a mechanism by which consumers can opt-out from receiving further email messages.

The spam messages direct consumers to different Web sites that sell products through deceptive means in violation of the FTC Act. Some Web sites sell a purportedly “100% safe and natural herbal” male enhancement pill. Not only do the pills not work as claimed, they are not “safe and natural.” The pills contain undisclosed prescription erectile dysfunction drugs that may be dangerous for certain users.

The spam also directs consumers to Web sites controlled by Defendants selling over 100 different “generic” versions of branded prescription drugs to treat various conditions, including depression, pain, and cholesterol issues. Defendants claim that the drugs come from a bona fide U.S. licensed pharmacy that dispenses FDA-approved generic drugs. In fact, Defendants do not operate a U.S. licensed pharmacy. They sell drugs that are shipped from India, have not been approved by the FDA, and are potentially unsafe. Moreover, the Web sites falsely claim that they provide a secure Internet connection for consumers that provide Defendants with their credit card numbers and health information.

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 hide their illegal practices by utilizing anonymous Web sites and spam. They have utilized shell companies in the British Virgin Islands and Cyprus, have purchased Internet services using false information, and have used

credit card processors in Cyprus and the Republic of Georgia. Moreover, they control overseas bank accounts and regularly convert funds into digital currency accounts. Tellingly, this district court previously entered a permanent injunction ordering Lance Atkinson to cease making false claims about “herbal” products and utilizing illegal spam messages. Defendants’ pattern of fraud, as well as their rampant attempts to conceal their identity, indicates that they are likely to hide assets if they receive notice of this action.

## **II. DEFENDANTS’ ENTERPRISE**

### **A. Defendants**

Defendants are two individuals – Lance Atkinson in Australia, and Jody Smith in the United States – and the companies that they own or control.<sup>1</sup>

Lance Atkinson is a New Zealand citizen who presently lives in Australia. Atkinson is the sole director and shareholder of Inet Ventures Pty Ltd., an Australian company. (PX 1 ¶ 8, Att. A.) In June 2005, the FTC obtained a \$2.2 million judgment and injunctive relief against Atkinson for selling worthless dietary supplements through illegal e-mail messages. *See FTC v. Global Web Promotions*, 04 C 3022 (N.D. Ill.). (PX 1 ¶ 97, Att. PP.)<sup>2</sup> As described below, Lance Atkinson has been involved in this operation since at least October 2006. He is responsible for all of the deceptive product claims and the illegal spam e-mail messages.

Jody Smith is a resident of Texas. Smith is the sole officer and shareholder of Defendant Tango Pay Inc. and Defendant Click Fusion Inc. -- both Delaware corporations. (PX 1 ¶¶ 10, 11, Atts. B, C.) TwoBucks Trading Limited (“TwoBucks”) is a company registered in Cyprus. (PX 7, ¶ 7.F.i.) Although Jody Smith is not a registered officer or director of TwoBucks, he controls financial accounts for the company. (PX 7 ¶ 7.F.i, Att. A at EPA9540; PX 1 ¶ 81.) As described below, Jody Smith became involved in this operation in or before December 2007. He is legally responsible for the illegal spam messages, and the evidence ties Jody Smith and his companies to the deceptive marketing of “generic” prescription drugs.

---

<sup>1</sup> This Court has personal jurisdiction over Defendants, and venue is proper. Under the FTC Act’s nationwide service of process provision, 15 U.S.C. § 53(b), “the relevant question becomes whether the person has minimum contacts with the United States.” *FTC v. Cleverlink Trading Ltd.*, No. 05 C 2889, 2006 WL 1735276, at \*4 (N.D. Ill. June 19, 2006) (Kendall, J.). Moreover, under to the FTC Act, an action may be brought where a corporation or person “resides or transacts business.” 15 U.S.C. § 53(b). Here, Defendants have advertised and sold products in this district. (PX 1 ¶¶ 31-34, 36-41, 42-49 (undercover purchases of Defendants’ products in this district); *Id.* ¶¶ 55-59 (records of telephone calls from consumers in this district to Defendants’ customer service telephone numbers). In addition, three of the six defendants are aliens who are subject to venue in any district.

<sup>2</sup> This case involves claims for different products, includes additional parties, and seeks immediate relief. Thus, the FTC is not at this point moving for contempt sanctions against Atkinson.

## **B. The Enterprise**

Defendants operate one of the biggest spam organizations in the world -- "Affking." The enterprise relies on a group of individuals -- many of whom have been recruited by Lance Atkinson -- who send anonymous bulk e-mail messages. The "spam" messages contain a link that, if clicked, directs consumers to one of various Web sites selling Defendants' products. Consumers pay for the products by credit card. Proceeds from the credit cards sales go to financial accounts controlled by Defendant Jody Smith. Smith uses the money to pay various third parties for services necessary to continue the operation, to pay commissions to the spammers who generate sales, and, ultimately, to pay himself and Atkinson.

The present enterprise is an outgrowth of an operation that began around October 2006. Lance Atkinson teamed up with his brother, Shane, a New Zealand citizen, who sold herbal products under the name "Genbucks." Operating as "Sancash," Lance Atkinson recruited and paid spammers to generate sales of the Genbucks herbal products, including a "hoodia" diet pill and "male enhancement" pill, as well as "replica" watches. In December 2007, New Zealand law enforcement officials executed search warrants on New Zealand locations connected to the Genbucks operation, including the home of Shane Atkinson. (PX 2 ¶ 12.) Lance Atkinson subsequently cut ties with his brother and began operating with Jody Smith under a new name -- "Affking." The Affking operation has continued to sell "male enhancement" pills and "replica" watches. In addition, the operation sells "generic" prescription drugs. The operation is ongoing, and the products continue to be promoted through spam e-mail.

### **1. Sancash**

Lance Atkinson, operating as "Sancash," sold "herbal" products and hired spammers to promote the products from approximately October 2006 through December 2007. Atkinson's own statements from online chat communications obtained by the New Zealand law enforcement agents during their searches, along with other evidence, confirm that:

- Lance Atkinson entered into an arrangement with his brother Shane and his company, Genbucks, whereby Lance Atkinson would receive a percentage of the sales that his affiliates generated for herbal products (PX 2 ¶¶ 18, 26-29, Att. B at p. 134);
- Using a nickname, Lance Atkinson posted messages on a pro-spam Internet bulletin board seeking affiliate "mailers" to promote the herbal pills (PX 1 ¶¶ 13-14, Atts. D, E);<sup>3</sup>

---

<sup>3</sup> Although Atkinson used an alias on the Internet bulletin board, he provided an ICQ online chat address. Records from Internet service providers demonstrate that Lance Atkinson logged into that ICQ account. (PX 3 ¶ 2, Att. A, at AOL4-5, 13-17; PX 2 ¶¶ 5-6; PX 5 ¶¶ 4-5.)

- Atkinson recruited an individual named Roland Smits who had assisted him in the *Global Web Promotions* operation to assist him in this enterprise. In one online chat discussion, Smits thanked Atkinson for inviting him back into the business and said “don’t wanna [mess] it up this time.” Atkinson responded: “lol [laugh out loud] well hopefully [it] doesn’t end in the FTC again.” (PX 2 ¶¶ 18, 26-29, Att. B, at p. 6);
- Lance Atkinson operated a password protected Web site called sancash.com where affiliate mailers could go to see the products being promoted -- including “VPXL” male enhancement pills, a “hoodia” diet pill and “King Replica” watches -- and obtain statistics concerning the amount of sales that they had generated (PX 1 ¶¶ 15-18, 20-22, Atts. G, I, K);<sup>4</sup>
- Using false information, Atkinson registered Internet domain names -- addresses such as example.com -- from a German domain name registrar,<sup>5</sup> and these Internet addresses were included as links in the spam messages promoting the products identified on the sancash.com Web site (*id.* ¶ 92, Att. NN);
- Lance Atkinson understood that spammers were marketing the products (PX 2 ¶¶ 37, 43-48, 50: [Shane Atkinson] *hey lance . . . I have a dude in India who employs 50 people [sic] to manually spam people from gmail / hotmail etc, you wanna [sic] him [Lance Atkinson] sure, send me his contact*); (PX 2 ¶¶ 18, 26-29, Att. B at p. 63: [Lance Atkinson] *russians want to do some serious spamming this weekend*); and
- Atkinson controlled an ePassporte online digital currency account<sup>6</sup> in the name of New Pacific Resources -- a company registered in the British Virgin Islands (PX 7 ¶ 7.B.i, Att. A at EPA690)<sup>7</sup>-- and, between October 2006 and December 2007, that account: (1) received over \$1.7 million from the Genbucks account (PX 1 ¶ 67; PX 7 ¶ 7.B.), (2) transferred almost \$240,000 into Lance Atkinson’s Inet Ventures ePassporte account referencing “sancash” (PX 1 ¶ 68), and (3) transferred over \$1.8 million to other accounts referencing “sancash,” presumably for sales commissions by e-mailers (*id.*).

---

4 Acting undercover, the FTC was provided a user name and password for sancash.com. (PX 1 ¶ 15, Att. F.) The FTC has provided screenshots of the site. (*Id.* ¶ 16, Att. G.) The sancash.com site provided little contact information other than an e-mail address of sancash@gmail.com. (*Id.*, Att. G at p. 2) Records from Internet service providers demonstrate that Lance Atkinson logged into this e-mail account. (PX 4 ¶ 4, Att. A, at GMA5; PX 2 ¶¶ 5-6.)

5 Although the domain names were purchased with false information (PX 6 ¶¶ 2-5, Att. B), records from the domain name registrar and Internet service providers demonstrate that Lance Atkinson logged in and purchased the domain names (PX 6 ¶ 5, Att. B; PX 2 ¶¶ 5-6; PX 5 ¶¶ 4-5).

6 ePassporte offers online accounts which, once logged into, can be used to send or accept payments from other ePassporte account holders and to transfer money to and from a bank account. (PX 7 ¶¶ 2-3.) ePassporte also offers its users a virtual Visa card which can be used to make purchases online, and certain users also receive a physical card which can be used to withdraw funds from ATM machines and make in-store purchases. (*Id.*)

7 Although the ePassporte account was opened in the name of New Pacific Resources, records from ePassporte and Internet service providers demonstrate that Lance Atkinson logged into the account. (PX 1 ¶ 85; PX 7 ¶ 7.B.ii; PX 2 ¶¶ 5-6; PX 5 ¶¶ 4-5.)

Chat logs show that, in December 2007, a reporter for the BBC contacted Shane Atkinson, inquiring about his involvement in the spam operation. Shane sent Lance an online message saying: “I had bbc world call my home. i think you need to stop spamming asap.” (PX 2 ¶¶ 30-36, Att. C at p. 5.)<sup>8</sup> Lance later had the following chat conversation with Roland Smits:

7310	2007-12-16T05:11:39	<b>sancash1</b>	did u know mine and shanes name were mentioned on a big BBC show about spamming ? he kinda freaked out
7311	2007-12-16T05:11:54	<b>SanCa\$hSupport</b>	lol
7312	2007-12-16T05:11:56	<b>sancash1</b>	like a 30 min doco
7313	2007-12-16T05:12:04	<b>SanCa\$hSupport</b>	how do u feel about it
7314	2007-12-16T05:12:39	<b>sancash1</b>	well they sort of said that shane was the one responsible for spamming
7315	2007-12-16T05:12:57	<b>sancash1</b>	all the penis sites
7316	2007-12-16T05:13:11	<b>sancash1</b>	and the local cops are investigating
7317	2007-12-16T05:13:16	<b>SanCa\$hSupport</b>	oh
7318	2007-12-16T05:13:19	<b>SanCa\$hSupport</b>	hmm
7319	2007-12-16T05:13:33	<b>SanCa\$hSupport</b>	umm not too hot then
7320	2007-12-16T05:13:54	<b>sancash1</b>	nah, they go after the source and genbucks was the source
7321	2007-12-16T05:14:13	<b>SanCa\$hSupport</b>	i guess so... they'll never find you
7322	2007-12-16T05:14:56	<b>sancash1</b>	well they bought me up, but nothing linked to me, most i do is provide services for spammers

(PX 2 ¶¶ 18, 26-29, Att. B, at p. 162-63.)

As mentioned above, on December 17, 2007, New Zealand authorities executed search warrants on locations in New Zealand connected to the Genbucks operation. (PX 2 ¶ 12.) Soon thereafter, the sancash.com Web site stopped operating.

## 2. Affking

Since the New Zealand searches took place in December 2007, Lance Atkinson has teamed with Jody Smith and his companies, operating as “Affking.” The sancash.com Web site has been replaced with an essentially identical Web site at affking.com that contains much of the same language. (*Compare* PX 1 ¶ 22, Att. K at p. 2 [sancash.com] *with id.* ¶ 28, Att. P at p. 3 [affking.com].) The affking.com Web site promotes the same “VPXL” male enhancement pills and “King Replica” watches as sancash.com, and additionally promotes prescription drug Web sites called “Target Pharmacy” and “Canadian Healthcare.”

Credit card sales of the Affking products appear to be generating over \$500,000 a month.<sup>9</sup> The funds are filtered through several corporations in different countries controlled by

---

<sup>8</sup> The BBC published an article and radio piece on the operation. (PX 1 ¶ 21, Att. J.)

<sup>9</sup> Affking product purchases can be traced to three merchant accounts controlled by banks in Cyprus and the Republic of Georgia. (PX 1 ¶¶ 33, 40, 48, 52; PX 16 ¶¶ 2, 5-7, Att. A at VIS006-8.) Records from Visa reveal that the accounts are processing, on average, roughly \$500,000 per month. (PX 16 ¶¶ 2, 5-7.) Because the sites also accept MasterCard, product sales are likely much higher.

Jody Smith. First, funds from prescription drug purchases are deposited into a bank account in Cyprus in the name of Defendant TwoBucks. (PX 1 ¶¶ 62-63; PX 8.) Funds are then transferred from the TwoBucks account into: (1) a U.S. bank account of Jody Smith's company, Defendant Tango Pay, which received \$3.3 million between September 2007 and May 2008 from Cyprus bank accounts (PX 1 ¶¶ 60-61, 64-65; PX 9, Att. A); and (2) an ePassporte account in the name of TwoBucks, which Smith also controls.<sup>10</sup> Funds put in the Tango Pay bank account are transferred into a Tango Pay ePassporte account opened by Smith (PX 1 ¶¶ 60-61, 66, 71; PX 7, ¶ 7.D.i.; PX 8), and many of these funds are then transferred to another account opened by Smith in the name of Defendant Click Fusion (PX 1 ¶ 72; PX 7 ¶ 7.E.i.).

Jody Smith then uses the funds to pay Lance Atkinson, himself, and the same affiliates who were paid as part of the Sancash operation. Funds in the Tango Pay, TwoBucks, and Click Fusion ePassporte accounts have been withdrawn or transferred, as follows:

- the Tango Pay and TwoBucks accounts transferred over \$100,000, often identified as “aff\_k payment,” to the account of Atkinson's company, Inet Ventures Pty Ltd, during the first five months of 2008 (PX 1 ¶¶ 66, 69);
- Jody Smith has withdrawn almost \$200,000 during the last year out of the Click Fusion account from ATM machines located near his home (*id.* ¶¶ 66, 74-75); and
- the Tango Pay and TwoBucks accounts have made payments -- often identified as from “affking” or “aff\_k payments” -- to many of the same individuals who were paid from Lance Atkinson's New Pacific Resources account referencing “sancash” (*id.* ¶¶ 73, 77).

Jody Smith also has purchased services necessary to continue the Affking operation using a number of ePassporte accounts funded by Tango Pay and Click Fusion, but opened under the names “Gerald Causey” and “Nicholas Santos.”<sup>11</sup> Using the “Gerald Causey” account, Jody Smith purchased service for telephone numbers that appear on consumers' credit card bills when they purchase the Affking products. (PX 1 ¶¶ 33, 40, 48, 52, 55, 66, 78; PX 13 ¶ 4, Att. A at VON004-6.) Moreover, using the “Nicholas Santos” account, Jody Smith purchased Web site hosting and domain names for prescription drug Web sites promoted by Affking. (PX 1 ¶¶ 42, 47, 66, 79; PX 14, ¶ 3; PX 15 ¶¶ 2, 4-5; PX 7 ¶¶ 7.G.i, 7.I.i.)

---

<sup>10</sup> Although Jody Smith did not open the TwoBucks account, records from ePassporte show that the credit card provided for the account was sent to his home. (PX 7 ¶ 7.F.i., Att. A. at EPA9539-40.) Moreover, records from ePassporte and Internet service providers show that Smith regularly logs into the TwoBucks account. (PX 1 ¶¶ 80-81, 84; PX 7 ¶ 7.F; PX 10 ¶ 3; PX 11, Att. A at CHA002; PX 12 ¶ 3.)

<sup>11</sup> Records from ePassporte and Internet service providers demonstrate that Jody Smith logged into, and therefore had control over, the “Gerald Causey” and “Nicholas Santos” accounts. (PX 1 ¶¶ 80, 82-84; PX 7 ¶¶ 7.G, 7.I.; PX 11, Att. A, at CHA002; PX 12 ¶ 3.)

### III. DEFENDANTS' ILLEGAL BUSINESS PRACTICES

Defendants' Affking operation promotes male enhancement pills and prescription drugs by making false and unsubstantiated claims aimed at defrauding consumers. The products are promoted by illegal commercial e-mail messages that Defendants procure.

#### A. Deceptive Male Enhancement Claims

The Affking operation promotes an "herbal" male enhancement pill that does not work as claimed and is falsely represented to be "100% safe and natural." The product is sold on Web sites that often identify the product as "VPXL," although other names for the product are used. (PX 1 ¶ 31, Att. R.)<sup>12</sup> The pills cost \$59.95 plus \$17.95 shipping and handling. (*Id.* ¶ 32.) An undercover VPXL purchase was received from China. (*Id.* ¶ 34, Att. T.)

The Web sites falsely claim that the product is "100% natural with no known side effects" and "a 100% safe and natural herbal formula[.]" (PX 1 ¶ 31, Att. R at p. 3, 4.) In fact, the VPXL product that the FTC purchased undercover was tested by the FDA's Division of Pharmaceutical Analysis, and it was found to contain sildenafil, the active ingredient in Viagra. (PX 17 ¶¶ 2-4, Att. A.)<sup>13</sup> According to testimony submitted by the FTC from a urology expert, a supplement containing sildenafil cannot be considered 100% safe and could cause significant side effects in certain individuals, even in small doses. (PX 18 ¶¶ 6-7, 15-22.)<sup>14</sup>

Furthermore, the sites falsely represent that the product permanently enlarges a man's penis. (PX 1 ¶ 31, Att. R.) There are no reputable scientific studies that support a claim that any dietary supplement can permanently enlarge the size of a man's penis. (PX 18 ¶¶ 6-7, 13-14.) The FDA has never approved any medication for enlarging a penis. (*Id.* ¶ 13.) No pill has been shown to be effective. (*Id.*) In short, any claim that a pill or dietary supplement can permanently enlarge a man's penis is completely false.

#### B. Deceptive Pharmaceutical Drug Claims

The Web sites and e-mail messages promoting Defendants' pharmaceutical drug Web sites falsely claim that their "generic" drugs are sold by a U.S. licensed pharmacy and approved

---

12 The product has also been called names including "ManSter" and "MegaDik." Online chats show that Lance Atkinson switched the product name from ManSter after it got a bad reputation on the Internet, and that he selected the name "VPXL." (PX 2 ¶¶ 18, 26-29, Att. B at pp. 136, 141-142.)

13 The FDA lab findings are consistent with testing done on VPXL by other countries. Health officials in both Denmark and Canada have issued public warnings about VPXL being adulterated with prescription erectile dysfunction drugs on their Web sites. (PX 1 ¶ 88, Att. LL.)

14 In particular, taking nitrates (which are found in many medicines used to treat diabetes, high blood pressure, or heart disease) together with erectile dysfunction drugs can lower blood pressure to an unsafe level, causing individuals to get faint or even have a heart attack or stroke. (PX 18 ¶ 20.)



by the FDA. The Web sites -- named “Target Pharmacy” or “Canadian Healthcare” -- sell over 100 different “generic” versions of brand name prescription medications, including drugs such as Levitra, Flomax, Viagra, and Lipitor. (PX 1 ¶¶ 37, 43, Att. V at pp. 11-42.) Undercover purchases reveal that the drugs come from India, and the packages consist solely of blister packs of pills. (*Id.* ¶¶ 41, 49, Atts. Y, FF.) Consumers do not receive a prescription, and there is no indication that there is a medical doctor involved in the dispensing of the drugs. (*Id.* ¶¶ 41, 49.) The pharmacy Web sites contain no contact information. (*Id.* ¶¶ 36, 43.)

**1. The operation falsely claims to be a bona fide U.S. licensed pharmacy**

The pharmacy sites claim that they are a bona fide U.S. pharmacy. The front page of the Web sites says:

Our pharmacies are licensed to ship medication to all countries in the world, and employ licensed pharmacists to provide you with the highest standards of pharmaceutical care. All medication is obtained from legitimate pharmaceutical wholesalers, so you can rest assured that you are receiving the same medication as you would at your neighborhood pharmacy.

(PX 1 ¶ 36, Att. V at p. 2.) In addition, the sites explicitly state in two locations: “We use only . . . U.S. licensed pharmacies.” (*Id.* at pp. 2, 6.)

In fact, Defendants do not operate a pharmacy licensed in the United States. Pharmacies in the U.S. are licensed by individual states. (PX 23 ¶ 5.) Testimony submitted from the National Association of Boards of Pharmacy, whose membership consists of the state pharmacy license boards, reveals, upon review of records of the license boards, that neither “Target Pharmacy,” “Canadian Healthcare,” nor any of the companies involved in the sale of the products, operate a licensed pharmacy in the United States. (*Id.* ¶ 8.) Instead, the enterprise is an unlicensed pharmacy that is operating outside of the law. (*Id.* ¶¶ 5, 8.)

**2. The operation falsely claims to sell FDA approved drugs**

The sites also claim to sell drugs approved for sale by the FDA. The sites claim:

**TARGET PHARMACY** is your convenient, safe and private online source for approved pharmacy prescriptions. We sell exact generic equivalents of US FDA approved prescription drugs through our fully-licensed pharmacies.

(PX 1 ¶ 36, Att. V at p. 4.) Elsewhere, the sites state the products are “approved by Indian FDA for export.” (*Id.* at p. 6.) In another place, the sites claim that users can “rest assured that you are receiving the same medication as you would at your neighborhood pharmacy.” (*Id.* at p. 2.)

The sites also contain a seal of the FDA under a statement that says “Our Awards.” Under the seal, the site says “Approved by American Drug Administration.” (*Id.* at p. 4.)<sup>15</sup>

In fact, testimony from an FDA representative confirms that many of the “generic” versions of brand name prescription drugs sold on the pharmacy sites are not approved by the FDA. The FDA has no records of any approval of generic versions of many of the drugs sold on the sites, including Levitra, Flomax, Viagra, Lipitor, and Crestor. (PX 22 ¶¶ 3-5.) Instead, these products are unapproved new drugs sold in violation of the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 355(a), 331(d). (PX 22 ¶ 5.) Thus, the drugs cannot be “the same medication” that consumers receive at “their neighborhood pharmacy.”

### **3. The operation makes false security claims**

Defendants’ pharmacy sites also falsely claim that they provide a secure Internet connection for consumers who provide Defendants with their credit card numbers and health information.<sup>16</sup> The pharmacy Web sites make explicit security claims. The sites claim to “treat your personal information (including credit card data) with the highest level of security.” (PX 1 ¶ 36, Att. V at p. 9.) Particularly, the sites claim (*see id.*):

when you place an order online your personal information is encrypted using SSL [Secure Socket Layer] encryption technology before being sent over the Internet. It makes it virtually impossible for your credit card details to be intercepted or stolen while being transmitted to our server.

In fact, the security claims are false. The pharmacy sites do not use SSL encryption. (*Id.* at p. 52.) Thus, consumers’ sensitive health and financial information is not provided with the “highest level of security,” as claimed by Defendants.

### **C. The Illegal Spam Messages**

Defendants are responsible for likely billions of illegal commercial e-mail messages sent by their Affkings affiliates promoting the “VPXL” male enhancement pills, “King Replica” watches and “Target Pharmacy” and “Canadian Healthcare.” Indeed, anti-spam organization Spamhaus presently identifies this group as the worst “spam gang” in the world. (PX 1 ¶ 89, Att.

---

<sup>15</sup> Some spam messages marketing the pharmacy Web sites also make explicit claims that the drugs sold are approved by the FDA. For example, certain e-mail messages have contained the following subject lines: “Impotence pills as approved by the FDA” and “Claim your FreeViagraPills from us, FDA Pharmacy Online!” (PX 1 ¶ 96, Att. OO at pp. 1-2.)

<sup>16</sup> Consumers who purchase prescription medication on the pharmacy Web sites must provide significant personal information, including name, address, e-mail address and credit card information. (PX 1 ¶ 38, Att. V at pp. 49-51.) In addition, the Web sites contain a “medical questionnaire [sic]” that requests “optional” information, including gender, date of birth, weight, height, current medical conditions, current prescriptions, and past surgeries. (*Id.*)

MM.) Consumers have forwarded over three million e-mail messages connected to this operation to an e-mail address at which the FTC accepts spam complaints. (*Id.* ¶¶ 90-91.) The FTC has submitted several examples of the spam as exhibits. (*Id.* ¶ 96, Att. OO.) As described in more detail below, all of the messages blatantly disregard one or more of the protections Congress provided in the CAN-SPAM Act, 15 U.S.C. § 7701.<sup>17</sup>

**1. Defendants’ spam falsifies information that would identify the real sender**

The spam messages employ several illegal methods to hide the source of the messages. First, the spam messages touting Defendants’ products insert the e-mail addresses of unwitting third parties in the “from” fields of the spam, a practice often referred to as “spoofing.”

Examples submitted to the Court include:

“From” Line	“From” E-Mail Address	Owner of Domain	Product
Arun	yremogtn@woodstockny.org	Woodstock, NY	Canadian Healthcare
eLvitra Cyails	frgodefro@nestle.com	Nestle Corporation	Canadian Healthcare
England	Gerdine-isunubak@hoover.com	Hoover Inc.	Canadian Healthcare
Margie Campbell	Preyedrw4@fedarb.com	Federal Arbitration, Inc.	VPXL
Big	Tonmauer_1982@la-archdiocese.org	Archdiocese of Los Angeles	VPXL
Christa Waters	christasnotty@angelcabrera.com	Official Website of Angel Cabrera	VPXL
Daren	daren-ivatyses@cfcbasa.org	Central Florida Council, Boy Scout of America	VPXL
Replica Watches	olga.mirabal@miami-police.org	Miami Police Department	King Replica
Rolex Watches	pettitje@atrc.navy.mil	U.S. Navy	King Replica

(PX 1 ¶ 96, Att. OO.) The practice of “spoofing” conceals the true identity of the sender and makes it seem that the spam is coming from a variety of innocent parties. Because the e-mail messages also fail to provide Defendants’ physical address, it is essentially impossible for a recipient of the e-mail messages to identify who is the responsible party. (*Id.* ¶ 96.)<sup>18</sup>

---

17 Congress passed CAN-SPAM after finding that spamming imposes significant costs on the e-mail system, which are passed along to subscribers in the form of higher prices and reduced convenience. *See* 15 U.S.C. §§ 7701(a)(3), (4). Congress found that unsolicited commercial e-mail messages -- most of which are fraudulent or deceptive in one or more respects -- threaten the convenience and efficiency of e-mail, an “extremely important and popular means of communication.” *Id.* at §§ 7701(a)(1), (2).

18 Spoofing an e-mail message’s return path causes real harm to individual users and

Second, security researchers have found that many of the messages touting Affking products are routed without authorization through a vast number of compromised computers, often called a “botnet.” (PX 20 ¶¶ 9-13.)<sup>19</sup> In early 2008, a security company identified one botnet -- which it dubbed “Mega-D” -- that sent spam promoting Affking’s VPXL and King Replica products as the worst botnet in the world, accounting for 32% of all spam. (*Id.* ¶¶ 15-18, Att. A.) Security experts estimated that the botnet was capable of sending ten billion spam e-mail messages a day. (*Id.* ¶ 15.)

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

A key feature of CAN-SPAM is the requirement that commercial e-mail messages sent to consumers contain a mechanism that consumers can use to opt-out of receiving future messages. Defendants’ spam messages 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. (PX 1 ¶ 96, Att. OO.)

## 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 granted TROs in similar actions.<sup>20</sup>

---

Internet service providers. When spammers send out email messages, a number of them are undeliverable for various reasons. (PX 1 ¶ 95.) The flood of undeliverable spam 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 FTC has submitted testimony from an Internet service provider in Peru, Illinois whose customers -- including businesses, hospitals and police departments -- lost the ability to get incoming e-mail for days after the ISP was flooded with “bounced” messages for “King Replica” and “VPXL” spam messages. (PX 19 ¶¶ 2, 4-5, 7, 9, Att. B; PX 1 ¶ 93.) The situation was only resolved after the ISP purchased additional computer servers. (PX 19 ¶¶ 10-11.)

19 A botnet is network of computers that have been compromised, usually because owners open malicious e-mail attachments, follow links in spam, or visit Web sites exploiting vulnerable systems. (PX 20 ¶ 9.) A botnet “controller” can program the botnet to distribute spam. (*Id.* ¶ 10.)

20 *See, e.g., FTC v. Spear Systems, Inc.*, 07C 5597 (N.D. Ill. Oct. 5, 2007) (Andersen, J.) (*ex parte* TRO and asset freeze for violations of FTC Act and CAN-SPAM); *FTC v. Sili Neutraceuticals, LLC*, 07C 4541 (N.D. Ill. Aug. 13, 2007) (Kennelly, J.) (same); *FTC v. Cleverlink Trading Limited*, 05 C 2889 (N.D. Ill. May 15, 2005) (St. Eve., J.) (*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.) (*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.) (same); *FTC v. Stuffingforcash.com, Inc.*, 02 C 5022 (N.D. Ill. July 16, 2002) (Norgle, J.) (*ex parte* TRO and asset freeze for violations of FTC Act and commercial email marketing); *FTC v. TLD Network Ltd.*, No. 02 C 1475 (N.D. Ill. Feb. 28, 2002) (Holderman, J.) (same).

### **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). Under the Seventh Circuit’s test for injunctive relief, the threshold showing of likelihood to succeed 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 has established that Defendants have committed clear and repeated violations of the FTC Act by making material misrepresentations to consumers about their products and procuring the initiation of commercial e-mail messages that violate CAN-SPAM.

#### **1. FTC Act violations**

The false claims about the male enhancement products and the pharmacy services 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 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). 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. QT, Inc.*, 448 F. Supp. 2d 908, 957 (N.D. Ill. 2006); *Sabal*, 32 F. Supp. 2d 1004, 1007 (N.D. Ill. 1998). The FTC is not required to prove intent to deceive. *Bay Area*, 423 F.3d at 635.

As described in § III.A, the Web sites promoting the male enhancement pills make express representations that the pills are “100% safe and herbal” and that the pills will permanently increase the size of a man’s penis. In fact, the pills are adulterated with prescription erectile dysfunction drugs that are potentially harmful for certain individuals. In addition, medical testimony confirms that the pills do not work as claimed. In short, the claims made about the male enhancement pills are clearly likely to mislead consumers.<sup>21</sup>

---

<sup>21</sup> As noted above in Section II.B.1, Lance Atkinson previously promoted a hoodia diet pill. The Web sites touting hoodia -- which purports to be an African cactus plant -- claim that hoodia can reduce calorie intake “by up to 1000 calories a day,” equating to “4-6 pounds a week” (PX 1 ¶ 19, Att. H at p. 4.) Testimony from the Medical Director of the Northwestern Comprehensive Center on Obesity

Similarly, as set forth in § III.B above, the Web sites and e-mail messages promoting the “pharmacy” services make material false statements. First, the sites falsely claim that they operate a bona fide pharmacy licensed in the United States. Second, the sites falsely claim that they dispense FDA-approved generic drugs. Third, the sites falsely claim that they securely transmit sensitive health and financial information provided by consumers on the site. These claims are material because they imply to consumers the trustworthiness, security and safety of drugs and purchases on the “pharmacy” sites. Consumers understandably want to make sure that if they try to save money on drugs over the Internet that the drugs are the real thing and are safe for them. If consumers knew that the pharmacy was not licensed in the United States, dispensed drugs unapproved by the FDA, and did not provide the online security claimed on the site, their purchasing decision would clearly be affected.

## **2. CAN-SPAM Violations**

The CAN-SPAM violations in this case -- which, pursuant to CAN-SPAM, are violations of the FTC Act, *see* 15 U.S.C. § 7706(a) -- are well-documented and widespread.

- *False or misleading header information:* As described in § III.C.1, Defendants initiate commercial e-mail messages that falsify the originating e-mail address and are routed through compromised computers without authorization, impairing the ability of consumers and law enforcement to determine the sender’s true identity in violation of CAN-SPAM, 15 U.S.C. § 7704(a)(1).<sup>22</sup>
- *Failure to include opt-out mechanism:* As described in Section III.C.2, Defendants initiate commercial e-mail 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).
- *Failure to include a postal address:* Defendants’ commercial e-mail messages additionally fail to include a valid postal address in violation of CAN-SPAM, 15 U.S.C. § 7704(a)(5)(A)(iii).

## **3. Defendants are responsible for the illegal practices**

Despite their best efforts to hide their involvement in this operation, the evidence set forth above in § II.B demonstrates that Defendants control and profit from the illegal practices. The evidence shows that Defendants receive the proceeds of product sales and arrange for the

---

shows that these claims are false, and that hoodia cannot cause any weight loss absent a reduction in calorie intake or an increase in exercise. (PX 21 ¶¶ 7-8, 11.) Although Lance Atkinson does not appear to be promoting the hoodia product presently, the FTC also seeks an injunction against false claims concerning this product.

<sup>22</sup> CAN-SPAM defines “header information” to include the “source, destination and routing information . . . including the . . . originating electronic mail address[.]” 15 U.S.C. § 7702(8).

marketing of the products by paying e-mail marketers and purchasing other Internet services, including domain names and telephone service.

Under similar factual circumstances, Judge Holderman granted a preliminary injunction halting violations of the FTC Act and CAN-SPAM against parties profiting from anonymous e-mail messages and Web sites deceptively selling ineffective diet patches. *See FTC v. Phoenix Avatar*, No. 04 C 2897, 2004 WL 1746698 (N.D. Ill. July 30, 2004) (*See Attachment A*). In that matter, Judge Holderman noted (at \*12-13):

[T]he 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 Web sites] and also establishes that the money spent purchasing the diet patches ended up in the defendants' possession. . . . 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.

Here, the facts demonstrate that Defendants control and profit from the present operation. Chat logs and Internet bulletin board postings demonstrate that Defendant Lance Atkinson recruits spammers and provides services for them to send spam messages promoting the products at issue here. Financial records show that accounts controlled by Jody Smith in the name of Defendants TwoBucks, Tango Pay, and Click Fusion receive proceeds of product sales. Smith pays a portion of the profits to Atkinson (through Atkinson's company, Defendant Inet Ventures), pays himself, pays commissions to the spammers who generated sales, and pays for other Internet services related to this operation.<sup>23</sup>

#### **D. 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 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

---

<sup>23</sup> Lance Atkinson and Jody Smith also are individually responsible for the illegal activity here. 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; *World Travel*, 861 F.2d at 1031. Here, as explained above in Section II.B, each of the individual defendants has intimate knowledge and extensive participation in the business affairs.

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-VIII of the Proposed TRO contain conduct prohibitions to ensure future compliance with the FTC Act and CAN-SPAM. Sections IX-XIII 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.

**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 e-mail 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).

**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 (*see supra* p. 11, n. 20), there is a tangible risk that assets and evidence stemming from the illegal activity will disappear if Defendants receive prior notice. Defendants already have shown their ability to hide their identities. They use false addresses and routing information in their email messages. They utilize Web sites that provide no contact information.




They have used shell companies in the British Virgin Islands and Cyprus, purchased Internet services using false information, and used credit card processors in Cyprus and the Republic of Georgia. Moreover, they control overseas bank accounts and regularly convert funds into digital currency accounts. 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 by violating the FTC Act and CAN-SPAM. 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  
Federal Trade Commission  
55 W. Monroe St., Suite 1825  
Chicago, IL 60603  
Voice: (312) 960-5634  
Facsimile: (312) 960-5600

Date: October 6, 2008