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

FEDERAL TRADE COMMISSION,	)	
Plaintiff,	)	Case No. 05C 6737
v.	)	Judge William J. Hibbler
ZACHARY A. KINION,	)	Magistrate Judge Nan R. Nolan
Defendant.	)	

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

I. INTRODUCTION

The FTC seeks to stop Defendant Zachary Kinion from deluging consumers' email inboxes with junk email messages that violate federal law and cause significant injury to consumers and industry. Defendant is responsible for "spam" email messages advertising mortgage opportunities, adult entertainment, privacy software, and online pharmaceuticals. He goes to great lengths to cloak his identity, seeking to evade responsibility for the offending spam that he sends. Left unchecked, Defendant is likely to continue sending spam under the guise of anonymity, and he will continue to reap unjust rewards through illegal action.

Defendant's spam messages violate several provisions of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), 15 U.S.C. § 7701, *et seq*. The messages are illegally sent through computers of innocent third parties, and they contain forged information to make it appear that the messages were sent by others, such as the

U.S. Department of Defense and NASA. The spam frequently contains deceptive subject lines designed to fool consumers into opening messages they would otherwise delete. Finally, the spam does not provide consumers with an opportunity to opt-out of receiving future messages, and does not contain any valid contact information such as a postal address or an accurate return email address. The FTC has amassed thousands of examples of Defendant's offending spam, an amount that is likely only a tiny fraction of the total amount Defendant has sent.

The FTC respectfully requests that this Court enter a temporary restraining order ("TRO") bringing Defendant's practices to a swift end. The FTC also requests that the TRO preserve Defendant's assets to ensure that he does not dissipate or transfer the assets he obtained from this illegal spam operation. Without the requested relief, Defendant's illegal spamming operation likely will continue unabated.

II. JURISDICTION AND VENUE

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

Venue is proper in the Northern District of Illinois. Pursuant to the FTC Act, an action may be brought where a corporation or person "resides or transacts business." *See* 15 U.S.C. § 53(b). Defendant has transacted considerable business in this district. ((*See* PX 1 ¶ 7; PX 2)

(Defendant leased computer server in Chicago that sent illegal spam messages); (PX 1 ¶¶ 14-16, Att. G; PX 3; PX 4 ¶¶ 13-15) (illegal email messages routed through computers in this district)).

III. DEFENDANT'S "SPAMMING" BUSINESS

Defendant Zachary Kinion both sends illegal spam and pays others who send illegal spam to market products that he is selling.[1] 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] All of these illegal actions cause significant harm to consumers and Internet service providers.

A. Defendant Has Routed Illegal Spam Through A Third Party's Computer Without Authorization

Defendant has routed spam messages through at least one third party computer without authorization. Defendant leased a computer server in Chicago, and he was assigned an Internet connection, *i.e.*, an Internet protocol address ("IP address"). (PX 1 ¶ 7.) During August 2004, Defendant's IP address connected into a computer located in Indiana without authorization. (PX 2 ¶¶ 4-5.) Once connected into the Indiana computer, Defendant attempted to send over 1000

---

[1] As described *supra* at § IV.B.1, both transmitting spam and procuring spam subject Defendant to liability here.

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

commercial email messages. (*Id.* ¶ 5.) The email messages advertised pharmaceuticals and "adult DVDs." (*Id.* ¶ 6, Att. A.)

Relaying messages through vulnerable computers – many of which are simply personal computers with broadband connections operating without firewalls – is a way spammers can hide. (PX 4 ¶¶ 9-12.) Doing so obscures the routing information of an email message by identifying the sending computer as the computer that was used as a relay, in effect "laundering" the message. (*Id.* ¶¶ 11-12.) Spammers typically use this method to evade anti-spam efforts of the spam recipient or his or her Internet service provider. (*Id.* ¶¶ 6, 9-10.) Such practices can cause real harm to users whose computers are unwittingly used as a relay. First, when functioning as a spam relay, a computer will often be slower than normal (or unstable and more likely to crash than normal). (*Id.* ¶ 10.) Moreover, if an individual's computer is repeatedly used as a launching pad to send spam, the user could be terminated by his or her Internet service provider if spam complaints are linked to the user's machine. (*Id.*)

B. Defendant Has Paid Third Parties Who Send Illegal Spam To Market His Products Or Services

Defendant also has paid third parties to market products with illegal spam. During June and July 2004, Defendant paid third parties to send spam to promote an Internet privacy software program.[3] From late 2004 through at least March 2005, Defendant paid third parties to send

[3] Defendant purchased the website address evidence-term.com. (*See* PX 1 ¶ 9, Att. C.) Spam promoting Internet privacy software on the evidence-term.com website appeared in June and July 2004. (*Id.* ¶¶ 14-16, Att. G at MSN22-30.) During this time period, Defendant paid various third parties using the online payment processor PayPal, identifying the subject of the payment as "evidenceterm" or "Evterm." (*Id.* at ¶ 8(B)(iii-v).)

spam to promote mortgage opportunities.[4] Defendant recruited individuals to send spam by posting messages on the Internet bulletin board "spamforum.biz," which openly advertises that it assists individuals to "Make big money with spam." (PX 1 ¶ 19, Att. J.)[5] The FTC has identified thousands of spam messages that Defendant procured, and has submitted examples of the spam. (*Id.* ¶¶ 14-16, Att. G; PX 3.)[6] 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.

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

The spam messages employ a variety of illegal techniques to conceal the identity of the sender, a practice often referred to as "spoofing." First, the messages include forged "from" or "reply-to" email addresses. The "from" or "reply-to" email addresses that purportedly sent the messages – often random character strings such as iwghkmbioby@yahoo.com or

---

[4] Defendant purchased various website addresses, including www.gsvdvs.info, www.lpjsjfv.info, and www.gffefv.net. (*See* PX 1 ¶¶ 9-10, Atts. C, D.) Spam promoting mortgage opportunities available on these websites appeared in late 2004, and continued through at least March 2005. (*Id.* ¶¶ 14-16, Att. G at MSN4-21.) During the time period that spam promoted the mortgage websites, Defendant was paid by various mortgage brokers for generating mortgage leads (*see id.* ¶¶ 8(B)(vi-vii), 21-22), and he paid various third parties for identifying mortgage leads (*see id.* ¶ 8(B)(ix)).

[5] Defendant posted messages on the spamforum.biz site using the moniker "jarondi" and "jarondi99." (PX 1 ¶ 19(A).) Defendant similarly used the moniker "jarondi99" when paying individuals for mortgage leads (*id.* ¶ 8(B)(ix)), and he provided the email address jarondi33@gmail when paying for his privacy software and mortgage website addresses (*id.* ¶¶ 11).

[6] The FTC obtained the spam messages from a secure database run by Microsoft Corporation, which operates the free email service Hotmail. (PX 3 ¶ 1.) 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.* ¶¶ 3-5.)

ppwfvg@aol.com (*see* PX 1 ¶¶ 14-17, Att. H; PX 3) – were, in fact, not involved in the transmission of the email messages. (*See id.* ¶ 16.) In addition to obscuring the identity of the sender, using false "reply-to" addresses causes harm to the Internet server providers whose email addresses are misappropriated. (*Id.* ¶¶ 6-8.)[7]

Defendant's spam also often adds arbitrary, false routing information. For example, in some cases, the message has identified the spam message as having originated from, or been transmitted by, computers operated by NASA and the U.S. Department of Defense. (PX 4 ¶¶ 11, 17.) In fact, the messages were not transmitted by these entities, and the false information was likely inserted to fool filters to trust the messages that would otherwise be identified as unwanted spam and deleted. (*Id.* ¶¶ 6, 11-12, 17.)

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

The subject lines of email messages contain information that consumers use to evaluate whether to open the messages. The subject lines of many of Defendant's spam messages deceptively suggest that the recipients have a prior commercial relationship with the sender and that the messages are urgent. The messages include subject lines such as "Re: Your 2nd Notice # 4N8422" and "Re: Your Final No[t]ice # 5T9500." (PX 1 ¶¶ 14-16, Att G at MSN4-7.) In fact, Defendant does not have prior relationships with the recipients (*see* PX 3 (email messages sent to "trap accounts")), and the subject lines presumably are used to trick consumers into opening messages that they otherwise would delete.

---

[7] When spammers blast out email messages, a number of them are undeliverable because of wrong addresses or other reasons. (PX 4 ¶ 8.) The flood of undeliverable email message is returned to the "reply-to" address maintained by the innocent party, not the spammer, causing the innocent party to deal with additional bandwidth and transaction costs. (*Id.*)

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. Defendant's spam messages, however, fail to provide consumers with the opportunity to opt-out. Indeed, Defendant's spam messages invariably do not include *any* notification to recipients of their ability to decline receiving further email messages from Defendant. (*See, e.g.*, PX 1 ¶¶ 14-16, Att. G at MSN04-30.) Thus, once consumers receive unwanted messages, there is no mechanism by which consumers can stop the messages.

IV. ARGUMENT

Defendant's spamming operation violates almost every provision of the CAN-SPAM Act. He is responsible for a deluge of email messages to consumers who, because of Defendant's deceptive and illegal conduct, cannot stop the barrage of spam to their email inboxes. In order to protect the public from Defendant's illegal activities and to prevent Defendant from continuing to make unlawful profits, the FTC requests that the Court enter a TRO with ancillary equitable relief to ensure that the Court can grant effective final relief at the conclusion of this case.

A. Injunctive Relief Standard

A district court may issue injunctions to enjoin violations of the FTC Act. *See* 15 U.S.C. § 53(b); *FTC v. Febre*, 128 F.3d 530, 534 (7th Cir. 1997); *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1028 (7th Cir. 1988). To obtain a temporary restraining order, the FTC must merely demonstrate: (1) a likelihood of success on the merits, and (2) that the balance of the equities tips in its favor. *World Travel*, 861 F.2d at 1029. "[T]he FTC need not prove irreparable injury to obtain a preliminary injunction." *Kinney v. Int'l Union of Operating Eng'rs*,

994 F.2d 1271, 1277 (7th Cir. 1993). The threshold showing of a likelihood to succeed under the Seventh Circuit's test for injunctive relief is a better than negligible chance of success on the merits. *See Cooper v. Salazaar*, 196 F.3d 809, 813 (7th Cir. 1999). Courts in this district have repeatedly exercised their authority to grant TROs in similar FTC actions.[8]

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

The FTC alleges violations of the CAN-SPAM Act, 15 U.S.C. § 7701 *et seq.*[9] These violations are well-documented and widespread. Defendant is directly responsible for compliance with these laws and is directly liable for their systematic violation.

1. Defendant Is An "Initiator" of Commercial Email

Defendant is legally responsible for the email messages in this case. CAN-SPAM imposes liability for a commercial email message upon "initiators" of the email. 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. §

---

[8] *See, e.g., 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); *FTC v. International Research and Dev. Corp. of Nevada*, 04 C 6901 (N.D. Ill. Nov. 10, 2004) (Hibbler, J.) (granting TRO and asset preservation for violations of FTC Act); *FTC v. Harry, et al.,* No. 04 C 4790 (N.D. Ill. Aug. 10, 2004) (Manning, J.) (granting *ex parte* TRO with asset freeze for violations of CAN-SPAM and FTC Act); *FTC v. Phoenix Avatar LLC, et al.*, No. 04 C 2897 (N.D. Ill. April 23, 2004) (Holderman, J.) (granting *ex parte* TRO with asset freeze for violations of CAN-SPAM and FTC Act); *FTC v. Stuffingforcash.com, Inc.*, 02 C 5022 (N.D. Ill. July 16, 2002) (Norgle, J.) (granting *ex parte* TRO with asset freeze for violations of FTC Act for commercial 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).

[9] The FTC Act prohibits "unfair or deceptive acts or practices." 15 U.S.C. § 45(a). CAN-SPAM states that it "shall be enforced by the [FTC] as if the violation of this Act were an unfair or deceptive act or practice proscribed under Section 18(a)(1)(B) of the [FTC] Act." 15 U.S.C. 57a(a)(1)(B). A violation of a rule proscribed pursuant to 15 U.S.C. § 57a(a)(1)(B) is an "unfair or deceptive act or practice in violation of § 45(a)(1) [of the FTC Act]." *See* 15 U.S.C. § 57a(d)(3).

7702(9). CAN-SPAM defines procurers as those who "intentionally pay or provide other consideration to, or induce, another person to initiate" a message on their behalf. 15 U.S.C. § 7702(12). *See also FTC v. Phoenix Avatar*, No. 04C 2897, 2004 WL 1746698, at *13 (N.D. Ill. July 30, 2004) ("Liability [under CAN-SPAM] is not limited to those who physically cause spam to be transmitted, but also extends to those who 'procure the origination' of offending spam.").

Here, Defendant "initiates" the commercial email messages at issue. First, undoubtedly he is responsible for the email messages sent from his own Internet connection. (*See infra* § III.A.) Moreover, Defendant has procured others to send spam. (*See infra* § III.B.) The email messages direct consumers to websites that Defendant controls, and he has paid third parties to promote those websites. Under these circumstances, it is axiomatic that either Defendant sent the messages himself, or he procured someone to do it on his 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").

2. Defendant's Commercial Email Messages Violate CAN-SPAM

The evidence overwhelmingly shows that Defendant is responsible for commercial email messages violating CAN-SPAM. Defendant's commercial email messages: (1) utilize false or misleading header information; (2) mislead recipients as to the nature of the email through deceptive subject headings; (3) fail to include the opportunity to decline future email messages; and (4) fail to include the sender's postal address.

a. *False or misleading header information*

Defendant initiates 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).[10] As described above in § III.A, Defendant transmits spam through third parties' computers, falsifying the routing information of the message. As discussed in § III.B.1, Defendant initiates messages that contain forged "from" or "reply-to" email addresses and false routing information. This practice makes it difficult, if not impossible, for consumers and law enforcement to determine the sender's true identity. By initiating spam containing materially false and misleading header information, Defendant violates CAN-SPAM.

b. *Deceptive subject headings*

Defendant initiates 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 Defendant's spam like "Re: Your 2nd Notice # 4N8422" and "Re: Your Final No[t]ice # 5T9500" deceptively suggest urgency and a prior business relationship with the recipient – neither of which exist.

[10] CAN-SPAM defines "header information" as the "source, destination and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C. § 7702(8). For purposes of 15 U.S.C. § 7704(a)(1), "materially" includes "the alteration or concealment of header information in a manner that would impair the ability of . . . a law enforcement agency to identify, locate or respond to a person who initiated the e-mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message." 15 U.S.C. § 7704(a)(6).

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

Defendant initiates 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, Defendant violates this provision by initiating messages that do not contain *any* mechanism at all to decline future emails.

d. *Failure to include a postal address*

CAN-SPAM requires that senders provide a physical postal address where the sender can be reached. *See* 15 U.S.C. § 7704(a)(5). A review of the email messages demonstrates that Defendant fails to include a valid postal address in violation of CAN-SPAM. (*See* PX 1 ¶¶ 14-16, Att. G.)

C. The Balance of the Equities Favors the FTC

The FTC respectfully requests that this Court enter a narrowly tailored TRO that brings Defendant's illegal practices to a swift end, and that preserves Defendant's assets in order to prevent ill-gotten gains from being dissipated or transferred. In fashioning appropriate injunctive relief, this Court has authority "to grant any ancillary relief necessary to accomplish complete justice[.]" *World Travel*, 861 F.2d at 1026; *see also Febre*, 128 F.3d at 534 (district court has authority in FTC action to "order any ancillary equitable relief necessary to effectuate the exercise of the granted powers"). If a district court determines that it is probable that the FTC will prevail on the merits, the court has a "duty to ensure that the assets . . . [are] available to make restitution to injured consumers." *World Travel*, 861 F.2d at 1031.

1. The FTC Seeks A Narrowly-Tailored TRO[11]

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-V of the Proposed TRO contains conduct prohibitions to ensure future compliance with CAN-SPAM and the FTC Act. Sections VI-VIII contain asset preservation and accounting provisions aimed at identifying and preserving monies obtained unlawfully by Defendant,[12] and identifying individuals or entities who have acted in concert or participation with Defendant. 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. Defendant has no legitimate right to continue unlawful conduct, dissipate his unlawful profits or conceal information needed to effectuate relief in this case.

2. The TRO Would Work No Valid Hardship on Defendant

The balance of equities tips strongly in the FTC's favor. The FTC's Proposed TRO would prohibit Defendant and his agents from sending commercial email messages that violate CAN-SPAM and preserve assets for equitable monetary relief. The TRO would work no valid hardship on Defendant, as he has no right to engage in, or profit from, practices that violate the law. In balancing equities, the Court must assign "far greater" weight to the public interest advanced by the FTC than to any of Defendant's 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

---

[11] The FTC has submitted a Proposed Temporary Restraining Order with its papers.

[12] The Proposed TRO asset preservation provision (§ VI) allows Defendant to pay up to $3,000 per month for actual, ordinary and necessary living expenses.

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).

V. CONCLUSION

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

Respectfully submitted,

William Blumenthal
General Counsel

/s Steven M. Wernikoff

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

Dated: November 30, 2005