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

(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 pr

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

. C41_1 5T

[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 a Id. lTd(

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 ,wBT/T1_0 1 Tf0.0055.0 Td(i c(at le8142.175 0 Tdes¶ 1.) -0.0055 Tw 8.024l whe)Tj4.Tf-0.0055 Tc

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. transmittedrignicasead(nd t(

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

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.

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 urgencyBT/T1/i2ert005 Tc -9/T1likely to mislead a re

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 R.

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