WO

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Cyberheat, Inc., Defendant.	)	CV-05-457-TUC-DCB **ORDER**

Plaintiff's Motion for Summary Judgment and Defendant's Motion for Partial Summary Judgment are pending before the Court.

SUMMARY

This action involves enforcement by the Plaintiff Department of Justice, on behalf of the Federal Trade Commission (FTC), of the CAN-SPAM Act (2003)[1] (Act or Statute), and Adult Labeling Rule (Rule) (May 2004), specifically enforcement of the requirement to place warning labels on commercial electronic mail (email) that contains sexually explicit material. 15 U.S.C. §7704 (a) and (d); 16 C.F.R. §316.4. Plaintiff is seeking civil penalties of up to $11,000 for each violation (Section 5(m)(1)(A) of the FTC Act), a permanent injunction to prevent future violations (Section 13(b) of the FTC Act), and other equitable relief against Defendant.

Defendant is an Arizona corporation, Cyberheat, Inc., in the business of offering sexually explicit websites for consenting adults to view by subscription

[1]Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.

on the Internet. Cyberheat utilizes a promotional program called TopBucks in which affiliates enter into a contract arrangement with Cyberheat to promote its websites. The affiliate is compensated by Defendant for each successful contact with a Cyberheat website.

In a nutshell, Plaintiff alleges that ten of Defendant's affiliates sent a total of 642 sexually explicit, unconsented to, emails in violation of the Act and were paid a total of $209,120 in commissions within a one year period. During that same time period, Defendant lodged upwards of 400 complaints of computer users who received unwanted sexually explicit emails, with approximately 300 of those complaints coming from a single Defendant's affiliate. Plaintiff contends that Defendant did not screen affiliates, supplied affiliates with pornographic promotional materials, did not monitor or oversee its affiliates' promotional activities, and did not readily terminate affiliates after complaints of uninvited sexually explicit spam.

Defendant argues that it did not initiate the violative emails, as the Amended Complaint alleges. Defendant contends that it did not intend, nor is there any evidence that Cyberheat intended, that affiliates violate the Statute to promote its website. Defendant further argues that the affiliates acted independently and not as the alter ego of Cyberheat and to find Cyberheat in violation of the Act and the Rule for the acts of these independent affiliates is an overly broad, unintended blanket application of the Statute.

PROCEDURAL BACKGROUND

On July 20, 2005, Plaintiff filed a Complaint and on August 30, 2005, filed an Amended Complaint for Civil Penalties, Permanent Injunction and Other Equitable Relief. On September 19, 2005, Defendant filed an Answer. On November 8, 2005, a Scheduling Order was entered by the Court.

On July 28, 2006, Plaintiff filed a Motion for Summary Judgment (PMSJ), a Memorandum in Support(PMEM), and a Statement of Facts in Support (PSOF). On July 28, 2006, Defendant filed a Motion for Partial Summary Judgment (DMSJ) and a Statement of Facts in Support (DSOF).

On August 28, 2006, Plaintiff filed a Response in Opposition. On August 28, 2006, Defendant filed a Response in Opposition. In addition, Defendant filed an Objection to the Himelfarb Declaration. On September 12, 2006, both parties filed Reply briefs.

Oral argument by the parties was heard by the Court on December 12, 2006. The Court took the matter under advisement and requested the Plaintiff to file a Proposed Permanent Injunction for review. Plaintiff filed a Proposed Permanent Injunction on December 27, 2006. On January 11, 2007, Defendant filed a Memorandum in Response (SuppResp). On January 19, 2007, Plaintiff filed a Reply and a Revised Proposed Permanent Injunction.

DISCUSSION

A. Interpretation of the Statute

"Statutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.,* 469 U.S. 189, 194 (1985). The Court may consider how a word or phrase is used elsewhere in the same statute, or how it is used in other statutes, *Kungys v. United States*, 485 U.S. 759, 770 (1988), how the possible meanings fit within the statute as a whole, *United States v. Fausto*, 484 U.S. 439, 449-51 (1988), and may rely on the interaction of different statutory schemes to determine statutory plain meaning, so that statutes dealing with similar subjects may be interpreted harmoniously. *Jett v. Dallas Ind. Sch. Dist.*, 491 U.S. 701, 737 (1989).

The text of 15 U.S.C. §7704(d)(Statute), reads in pertinent part, as follows:

> (d) Requirement to place warning labels on commercial electronic mail containing sexually oriented material
>
> (1) In general
>
> No person may initiate in or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and--
>
> **(A)** fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection; or
>
> **(B)** fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only--
>
> **(i)** to the extent required or authorized pursuant to paragraph
>
> (2), any such marks or notices;
>
> **(ii)** the information required to be included in the message pursuant to subsection (a)(5) of this section; and
>
> **(iii)** instructions on how to access, or a mechanism to access, the sexually oriented material.

The text of the Adult Labeling Rule (Rule), 16 C.F.R. § 316.4, reads as follows:

> (a) Any person who initiates, to a protected computer, the transmission of a commercial electronic mail message that includes sexually oriented material must:
>
> (1) Exclude sexually oriented materials from the subject heading for the electronic mail message and include in the subject heading the phrase "SEXUALLY-EXPLICIT”: in capital letters as the first nineteen (19) characters at the beginning of the subject line; ...
>
> (2) Provide that the content of the message that is initially viewable by the recipient, when the message is opened by any recipient and absent any further actions by the recipient, include only the following information:
>
> (i) The phrase "SEXUALLY-EXPLICIT”: in a clear and conspicuous manner; ...

(ii) Clear and conspicuous identification that the message is an advertisement or solicitation;

(iii) Clear and conspicuous notice of the opportunity of a recipient to decline to receive further commercial electronic mail messages from the sender;

(iv) A functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that–

(A) A recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and

(B) Remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message;

(v) Clear and conspicuous display of a valid physical postal address of the sender; and

(vi) Any needed instructions on how to access, or activate a mechanism to access, the sexually oriented material, preceded by a clear and conspicuous statement that to avoid viewing the sexually oriented material, a recipient should delete the e-mail message without following such instructions.

(b) Prior affirmative consent. Paragraph (a) of this section does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

To violate the Statute, first one must "initiate in or affect interstate commerce." Section 7704. The Statute defines those and other applicable words in Section 7702, as follows:

(9) Initiate

The term "initiate," when used with respect to a commercial electronic mail message [email], means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message.

* * *

(12) Procure

The term "procure," when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf.

***

(16)(A) Sender

A person who initiates such a message and whose product, service, or Internet website is advertised or promoted by the message.

The *Oxford English Dictionary* (2007) defines "initiate" to "begin, commence, enter upon; to introduce, set going, give rise to, originate, start." The Senate Report[2] recommending the Statute for enactment states, with reference to the definition of "initiate," that "more than one person may be considered to have initiated a message, thus, if one company hires another to handle the tasks of composing, addressing, and coordinating the sending of a marketing appeal, both companies could be considered to have initiated the message-one procuring the origination of the message; the other for actually originating it." (S.Rep. 108-102, 2004 U.S.C.C.A.N. 2348.)

Black's Law Dictionary (8th ed. 2004) defines "procure" "as one who induces or prevails upon another to do something, esp. to engage in an illicit sexual act." The *Oxford English Dictionary* defines "procure" as "to try to induce; to urge, press; to induce or prevail upon someone to come; to bring, lead." The Senate Report explains the definition, as follows:

> when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or induce another person to initiate the message on one's behalf, while knowingly or consciously avoiding knowing the extent to which that person intends to comply with this Act. The intent of this definition is to make a company

---

[2] "Committee reports are the most frequently cited and relied-upon sources of legislative history, and in the Court's traditional view the most authoritative source. 'A committee report represents the considered and collective understanding of those Congressmen involved in drafting and studying proposed legislation. Floor debates reflect at best the understanding of individual Congressmen. It would take extensive and thoughtful debate to detract from the plain thrust of a committee report …' Committee reports are often the best evidence of bicameral agreement, either because the House and Senate reports are identical, or because a conference report explicates the chambers' resolution of differences." 2A *Sutherland Statutory Construction* § 48A:11 (6th ed.).

> responsible for an email message that it hires a third party to send, unless that third party engages in renegade behavior that the hiring company did not know about. However, the hiring company cannot avoid responsibility by purposefully remaining ignorant of the third party's practices. The 'consciously avoid knowing' portion of this definition is meant to impose a responsibility on a company hiring an email marketer to inquire and confirm that the marketer intends to comply with the requirement of this Act.

(S.Rep. 108-102. 2004 U.S.C.C.A.N. 2348.).

The legislative history leading to the promulgation of the CAN-SPAM Act reveals that:

> The purposes of this legislation are to: (i) prohibit senders of electronic mail (e-mail) for primarily commercial advertisements or promotional purposes from deceiving intended recipients or Internet service providers as to the source or subject matter of their e-mail messages; (ii) require such e-mail senders to give recipients an opportunity to decline to receive future commercial e-mail from them and to honor such requests; (iii) require senders of unsolicited commercial e-mail (UCE) to also include a valid physical address in the e-mail message and a clear notice that the message is an advertisement or solicitation; and (iv) prohibit businesses from knowingly promoting, or permitting the promotion of, their trade or business through e-mail transmitted with false or misleading sender or routing information.
>
> * * *
>
> Pornographic spam is more likely than other spam to contain fraudulent or misleading subject lines. In its recent report, the FTC found that more than 40 percent of all pornographic spam either did not alert recipients to images contained in the message or contained false subject lines, thus "making it more likely that recipients would open the messages without knowing that pornographic images will appear." Unsuspecting children who simply open e-mails with seemingly benign subject lines may be either affronted with pornographic images in the e-mail message itself, or automatically and instantly taken-without requiring any further action on their part (like clicking on a link)-to an adult web page exhibiting sexually explicit images.
>
> * * *
>
> Spam also is used to lure unwary users to websites that contain viruses, spyware, or other malicious computer code. Late last year, for instance, an Internet adult entertainment company created a "Trojan horse" program that was downloaded to unsuspecting users computers. Users were tricked into accepting the program through a spam message that promised to deliver an electronic greeting card. The downloaded program, however, instead routed users to the company's pornography websites.
>
> * * *
>
> Also common is spam with pornographic content or links to websites with pornographic content, which many recipients find offensive and

> which places additional burdens on parents to constantly monitor their children's email.
>
> * * *
>
> Pornographers, long on the cutting edge of technology, have taken to employing increasingly brazen techniques to sell their products and services. As mentioned above, the FTC estimates that 18 percent of all spam is pornographic or "adult-oriented" material. While not all of such spam[3] contains images, spammers often do send graphic sexual images embedded in the body of spam so that simply upon opening the e-mail message, a user is assaulted with explicit photographs or video images. More frequently, though, spam contains HTML code and a JavaScript applet that together automatically load a pornographic web page as soon as the spam message is either opened or, in some cases, simply "previewed" in certain e-mail programs preview panes.

See S. REP. 108-102, 2004 U.S.C.C.A.N. 2348[4].

In this action, the violative activities of the affiliates and the affiliates' relationship to Cyberheat are the primary issue. Neither the Statute nor the Rule contains the word "affiliate." The *Oxford English Dictionary* defines "affiliate" as "a recognized auxiliary, as an affiliated organization." *Black's Law Dictionary* defines "affiliate" as "a corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or a sibling corporation; one who controls, is controlled by, or is under common control with an issuer of a security."

Plaintiff's position is that Defendant acted as an initiator, sender and/or procurer, as defined in the Statute, and is directly liable for violations of its affiliates.

Here, Defendant argues that it had no control over the affiliates on how, when, or even if they ever promoted Defendant's website and that the Statute does not apply to this situation. The Terms and Conditions Agreement entered into by

---

[3]Spam is unsolicited commercial bulk electronic mail.

[4]SENATE REPORT NO. 108-102 (July 16, 2003, Sen. McCain, Committee on Commerce, Science, and Transportation).

affiliates was explicit that violations of the CAN-SPAM Act would not be tolerated and email promotions were not encouraged. Defendant argues that the facts do not support respondeat superior liability or vicarious liability. Defendant further argues that it did not have the ability to monitor or supervise the methods affiliates used to promote their website. "Since Cyberheat did not authorize its affiliates to use its promotional materials in emails, and since Cyberheat did not authorize its affiliates to send emails on Cyberheat's behalf, and since nothing in the contractual relationship provided the affiliates the power to do either on behalf of Cyberheat, the only remaining possibility for extending liability to Cyberheat for the acts of the affiliates is if the affiliates had the apparent authority to send the emails on Cyberheat's behalf." (SuppResp at 5.)

The text of the Statute plainly contemplates a situation where one entity or person either pays for or otherwise induces another person or entity on their behalf to send a violative email such that a joint violation of the Statute has occurred. The Statute states specifically that more than one person may be considered to have initiated a particular message. The text also makes it clear that procuring involves somehow inducing, either by money or otherwise, as part of the initiation of the particular message.

The CAN-SPAM Act was not enacted in a vacuum. Congress was compelled to enact a Statute to protect the Internet-using public from uninvited, unwanted sexually explicit email "by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet," because "[u]nsolicited commercial email, commonly known as spam, has quickly become one of the most pervasive intrusions in the lives of Americans."[5] A portion of that Statute deals specifically with sexually explicit materials otherwise known as

[5]S. Rep. 108-102, 2004 U.S.C.C.A.N. 2348.

pornography. What precipitated the focus on pornography was not the availability of pornography to consenting adults, but the unexpected, uninvited pornographic spam email messages that appear with no warning in plain view of anyone using the Internet at the time, from a nine-year-old student studying for a history test to an 80-year-old great aunt looking to send a greeting card. The Statute creates a legal obligation, a duty, assigned to those who are in the business of sending sexually explicit materials over the Internet. The duty is owed to the public, particularly those members of the public who use the Internet but do not consent to view sexually explicit materials. Reasonable care must be taken to ensure that those members of the public who do not chose to view sexually explicit materials on the Internet are not involuntarily subjected to those materials. The Act and the Rule are very specific about the reasonable care required to prevent uninvited pornographic Internet intrusions. It is foreseeable that when sexually explicit promotional materials are supplied to third parties, violations of the Act and Rule may occur. A duty of care arises when it is foreseeable that harm may result if care is not exercised. See, e.g., *Salinas v. United States*, 9 Fed. Appx. 662 (9th Cir. 2001). It is foreseeable that harm may result if care is not exercised here, particularly because of the nexus between the third party violations and the sexually explicit promotional materials provided by the company. The doctrine of vicarious liability applies to the enforcement of this portion of the Statute, because of the burden of the duty imposed on the provider of pornography on the Internet. Vicarious liability is the exception to the normal principal of individualized fault. It is liability imposed on one person for the harm caused by another because the duty is so important that is it not delegable or delegable at the peril of the duty holder. Further, the regulation of sexually explicit spam is unique and distinguishable from fraudulent or misrepresentative materials regulated by the

Act. To experience the violation derived from fraud and misrepresentation contained in an unsolicited email message requires review and consideration of the content, unlike the viewing of uninvited, unsolicited pornography which results in immediate harm.

The Statute directly applies to Cyberheat, as a provider of sexually explicit materials[6] for viewing on the Internet. Cyberheat maintains that a strict liability approach is not what the Statute contemplates and the Court agrees, for now. Cyberheat is a business and the Court will balance Cyberheat's economic needs (burden of the duty) with the need to enforce the Statute for the benefit of the public (foreseability of the harm). Here, the Court does not find the Statute applicable to a business such as Cyberheat for an accidental or mistaken violation, immediately attended to and corrected. By the same token, Cyberheat cannot insulate itself from any liability for the actions of the affiliates on its ultimate behalf and for its financial benefit purely by putting on blinders or inattention to monitoring and supervising the use of its sexually explicit materials.[7] Cyberheat has a duty that it can only delegate at its own peril. In the end, Cyberheat is paying affiliates who are successful in promoting Cyberheat and bringing in business to the company. Because Defendant is a purveyor of that which the Statute explicitly attempts to regulate, sexually explicit materials available on the Internet, the Court does view Defendant as having a duty to oversee the use of those sexually explicit materials when distributed for promotion, and despite the disclaimers, upon receipt of knowledge

---

[6]Plaintiff supplied the Court with examples of the violative sexually explicit emails in question and it would be fair to say that these emails consist of full page (top to bottom) pornography that leaves nothing to the imagination.

[7]In a case involving imputed negligence, liability will be imposed on one person for the negligence of another based on the relationship between the parties, or arising from a rule of statutory law, or contract...Essentially the negligence of one person will not be imputed to another unless there exists a legal obligation to respond to the other's fault. 57B *Am.Jur. 2d Negligence* §1096.

that affiliates were using their promotional literature in a violative manner, incurred a duty to act reasonably to stop that activity. Here, control over the affiliates and knowledge of the violations of the affiliates are two issues that are pivotal.[8]

In sum, the Court finds that the Act and Rule apply to the relationship between Cyberheat and its affiliates, such that the company may be held vicariously liable for the actions of the affiliates[9], depending on a resolution of the facts concerning control and knowledge.

B. Dispositive Motions

1. Legal Standard

Summary judgment is proper "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed.R.Civ.P. 56(c)). The moving party bears the initial burden of demonstrating the absence of a genuine issue of material fact. *See Celotex Corp. v. Catrett,* 477 U.S. 317, 323 (1986). The moving party, however, has no burden to negate or disprove matters on which the non-moving party will have the burden of proof at trial. The moving party need only point out to the Court that there is an absence of evidence to support the non-moving party's case. *See id.* at 325.

---

[8]Other enforcement statutes enacted to protect the public have been applied based on the principles of vicarious liability: *Fare Deals Ltd. v. World Choice Travel.Com, Inc.*, 180 F.Supp.2d 678 (D.Md. 2001)(AntiCybersquatting/vicarious liability); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996)(copyright and trademark infringement/vicarious liability); and, *Hard Rock Cafe Licensing v. Concession Services, Inc.*, 955 F.2d 1143 (7th Cir. 1992)(Lanham Trademark Act/vicarious liablity). These cases involve a resolution of facts concerning control and knowledge.

[9]The doctrine of vicarious liability is based on the relationship between the parties, whereby it is deemed a matter of public or social policy that regardless of fault one party should be liable for the acts of the other. 57B *Am.Jur. 2d Negligence* §1097.

The burden then shifts to the non-moving party to "designate 'specific facts showing that there is a genuine issue for trial." ' *See Celotex Corp.,* 477 U.S. at 324 (quoting Fed.R.Civ.P. 56(e)). To carry this burden, the non-moving party must "do more than simply show that there is some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp.,* 475 U.S. 574, 586 (1986). "The mere existence of a scintilla of evidence . . . will be insufficient; there must be evidence on which the jury could reasonably find for the [non-moving party]." *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 252 (1986). In a motion for summary judgment, the evidence is viewed in the light most favorable to the non-moving party, and all justifiable inferences are to be drawn in its favor. *See id.* at 255. "Credibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are jury functions, not those of a judge . . . ruling on a motion for summary judgment." *Id.*

2. Plaintiff's Case

After a thorough and extensive investigation conducted by investigators at the FTC, Plaintiff filed an civil enforcement action against Cyberheat pursuant to 15 U.S.C. §7704 (a), (d) and 16 C.F.R. §316.4. In Count I, Plaintiff claims that Defendant's acts and practices violate 15 U.S.C. §7704(d) and 16 C.F.R. §316.4(a) by initiating transmissions of commercial email messages to protected computers that include sexually oriented material and fail to include the phrase "sexually-explicit" within the first nineteen characters; fail to include within the initially viewable content message, "sexually-explicit"; fail to include notice and opportunity to decline; fail to include physical postal address of Defendant; and include sexually oriented material within the initially viewable content of the message. In Count II, Plaintiff alleges that Defendant initiated these transmissions with email messages that advertised or promoted Defendant's

Internet web sites without the requisite notice or opportunity to decline. Count III alleges that same as above but that the messages failed to include Defendant's valid physical postal address.

The government contends that there are no material questions of fact precluding resolution of the dispositive motion and that Defendant may be found in violation of the Act and Rule based on the actions of its affiliates. The primary document in support of Plaintiff's case is the Allyson Himelfarb Declaration. Her Declaration is supported by attached documents which were filed electronically and are contained on a CD-ROM disc.

Himelfarb is an investigator with the FTC in the Division of Marketing Practices, Bureau of Consumer Protection. Her job is specifically to investigate persons/entities who may be violating the Act and Rule, and to do so she utilizes Internet search engines, electronic databases and a variety of other computer-based investigative tools. Himelfarb's Declaration and the attachments are intended to show conclusively the Cyberheat and the affiliates were connected, as well as Cyberheat's knowledge of its affiliates' activities.

Himelfarb began investigating Defendant, identified as an operator of an online affiliate program called TopBucks that promotes and advertises dozens of adult entertainment websites, in December 2004. The investigation was initiated when Cyberheat was identified as an adult website that was allegedly violating the Act and the Rule thorough email message promotions. These messages were identified by the FTC's spam database, as well as the "Hotmail trap accounts" maintained by Microsoft Corporation. Himelfarb's job was to peel away the layers to generally identify: the company that owned or registered the adult website promoted by the messages; where possible, the individual entity that physically sent the email messages (affiliate); how many different affiliates sent emails

on Cyberheat's behalf; how many emails each affiliate sent; and, the number of recipients to which the emails were sent.

Himelfarb reviewed the identified emails for specific violations: (1) was the phrase "sexually-explicit" in the subject line and initially viewable area of the message; (2) was there sexually explicit text or images within the initially viewable area of the message; (3) was there a notice to opt-out within the viewable area; and (4) was there a valid physical postal address for Cyberheat within the initially-viewable area. Microsoft responded to the FTC's requests for information about Cyberheat email messages caught in its Hotmail trap accounts. To identify each email message provided by Microsoft, it provided two files: one file in Internet email format, ".eml" and one file in a portable document format, ".pdf". The .eml files reflect the source code and the .pdf files preserve the content of the email messages. To peel away the layers, Himelfarb:

> [R]eviewed the source code of the .eml files in order to identify the Uniform Resource Locators or URLS contained in the email messages. The URL is a unique address of a specific file or webpage on the Internet. A URL is comprised of the name of the protocol to be sued to access the file (commonly called HTTP), a domain name that identifies a specific computer on the Internet and a pathname, a hierarchical description that specific location of the file on the computer. In the emails that [Himelfarb] reviewed, typically one URL identified the hyperlink that the recipient would click to access the adult website being promoted by the email message. This URL is commonly referred to as the hyperlink reference and is typically signified by the identified in an email message's source code. Microsoft used these hyperlink reference URLs to perform “web captures." The web captures preserved the web page that a user would be directed to upon clicking the hyperlink reference URL.

(PMSJMem, Ex. 1 at 3.)

If the .pdf contained sexually explicit material, then Himelfarb checked to see whether the email violated the Act and the Rule. She then used the .eml to identify the course code for the message. She used Microsoft's web capture

to trace the website as registered to Cyberheat. The Microsoft web capture also identified the affiliate with an affiliate ID assigned to the affiliate by Cyberheat, in order for her to connect that affiliate's activity back to Cyberheat.

Some identified emails were not captured by Microsoft. In that case, Himelfarb clicked on the hyperlink contained in the email message and preserved the web page or pages to which the hyperlinks redirected. Himelfarb reviewed hundreds of email messages sent by 10 of Cyberheat's affiliates. The results of these emails were saved either in .pdf or .eml formats, as well as in HTML format for certain messages, along with related web captures and other recordings on a CD-ROM filed with the Court. During discovery Cyberheat also produced a list of domain names and payment information.[10]

The Plaintiff's position is that money in the form of commissions to affiliates and profit in the form of new business to Cyberheat was the motive for the use of violative emails to promote Cyberheat's website. "Affiliates of the Topbucks program are paid to advertise Cyberheat's websites, earning money each time they refer a customer who subscribes to one of the Cyberheat's adult websites." (PSOF at 3.) In effect, affiliates that participated in the TopBuck program were paid a commission for traffic and sales to Cyberheat.

Plaintiff contends that there is sufficient evidence to find Cyberheat aware of and directly responsible for these violations. Plaintiff lists the following: Cyberheat's screening process for affiliates was not significant; it had a policy not to approve an affiliate application previously determined to be a cheater or spammer, yet it did not ask affiliates if they intended use email to promote; it assigned affiliates with a unique four or five digit number to

[10]Himelfarb's Declaration goes on to, in explicit detail, explain the layers connecting the violating affiliate emails to Cyberheat.

track sales and to determine payment as commission for sales; some entities had more than on affiliate account with Cyberheat; the company provided free webhosting, marketing and promotional tools to affiliates - all featuring the sexually explicit material available on the Cyberheat website; and, affiliates had the ability add a hyperlink to the promotional materials and use them in emails, so that when pressed, these hyperlinks went directly to the Cyberheat sexually explicit website being advertised. Cyberheat provided affiliates with hourly statistics on the number of sales and clicks they have generated, as well as 24 hour assistance in some form to affiliates.

The Plaintiff asserts that Cyberheat was aware that email was a source of promotion and that affiliates had the potential to send unlawful spam as a means to advertise Cyberheat. Cyberheat had a method to receive and review complaints about unwanted spam. Complaints were forwarded to a spam complaint email account. "Between May 14, 2004 and June 7, 2005, Cyberheat received over 400 complaints from individuals who received unwanted commercial email messages from Cyberheat affiliates promoting Cyberheat's websites." (PSOF at 8.) Cyberheat did not terminate every affiliate who was the subject of a complaint and in some cases, reinstated previously terminated affiliates. If one of an affiliate's accounts was terminated for violations, not all of that affiliate's accounts were terminated. Cyberheat's Terms and Conditions for affiliates stated that affiliates should not use or employ any form of mass unsolicited electronic mailings and had an informal unwritten policy that affiliates should not advertise by email. Cyberheat did not employ any of the monitoring methods that were identified in this informal policy which was only disclosed to a handful of affiliates. Cyberheat relied on the provisions in the Terms and Conditions to prevent violations, as well as the reservation to terminate affiliates who violated the law.

Plaintiff contends the Defendant misconstrues the knowledge/intent element of the Statute. "The Act does not require any showing of specific intent or knowledge for liability to attach. Rather, Cyberheat's procurement of violative emails makes Cyberheat liable for injunctive relief for violating the Act. Furthermore, while not necessary for injunctive relief, Cyberheat's actual or constructive knowledge of the violations was sufficient to make it liable for civil penalties." (PResp at 11.) "What is required to find Cyberheat liable under the Act is something less that actual knowledge that its affiliates are engaging, or will engage, in a pattern or practice that violates this Act. That knowledge may be required for a criminal violation, but this is not a criminal case. What is required is less than consciously avoiding knowing that its affiliates are engaging in, or will engage, in a pattern of practice that violates the Act." (Id., 17-18.) Plaintiff does not have to prove conscious avoidance, just that the violations did not occur by accident. According to Plaintiff, "Congressional intent to impose liability tin FTC enforcement actions against those who cause CAN-SPAM violations, regardless of their "knowledge of the violations, could hardly be clearer." (PResp at 14.) "Cyberheat's agreement with affiliates to provide advertising services foreseeably involved the affiliates/ use of on-line advertising including email. Cyberheat even knew that some of its affiliates were using spam to promote Cyberheat's websites." (PResp at 19.) "Cyberheat argues that for liability to attach the Act requires that Cyberheat paid its affiliates." (Id.) Defendant admits that it entered into agreements with the third parties whereby it paid those third parties a commission or finders fee for sales resulting from referrals by those third parties to Defendant's Web sites." (PResp at 11.) "Defendant attempts to draw a distinction between this practice and paying the third parties to market or advertise Defendant's websites. Defendant does not disagree with the Government

concerning the facts surrounding the relationship between Cyberheat and its affiliates, it merely argues that those facts do not make Cyberheat liable for the violations." (PResp at 11.)

3. Cyberheat's Defense

Defendant denies that it was an initiator, procurer or sender in violation of the Act. It also denies that it is in violation of the Act through the actions of its affiliates, who Defendant claims in turn have violated their agreements with Defendant by violating the law.[11]

Defendant argues that there are questions of fact precluding summary judgment in Plaintiff's favor: whether payment before the transmission of the violating email was required to show a violation of the Act; whether defendant actually allowed its affiliates to use its marketing tools in illegal emails, reflecting direct evidence of knowledge/intent; whether any terminated affiliates were ever reinstated; whether it was feasible for Defendant to monitor the activities of its affiliates[12]; and, whether there was affirmative consent to 21 of the purportedly violative emails.[13]

The true bone of contention comes when Defendant begins to argue its case that they should not be held responsible for the emails sent by the affiliates, also called the independent "Webmasters" by the Defendant. The contract between TopBucks, Cyberheat's promotional entity, and the third parties is called the

---

[11]The first eleven pages of Defendant's dispositive motion goes to emails sent by Defendant to persons who consented to acceptance of the emails. The Plaintiff agrees that none of those emails are violations of the Statute and were never part of the Amended Complaint. The only violative emails in question are the ones sent by Cyberheat's affiliates.

[12]Defendant's objection to the submission of the Himelfarb Declaration is overruled. It is not submitted as an expert opinion but merely a compilation of the results of an investigation.

[13]For purposes of this motion, Plaintiff waived those emails in lieu of pursuing this action on the remaining 600 or so at issue.

Terms and Conditions Agreement and specifically refers to the third parties as affiliates. Defendant's primary argument is that the "Defendant did not actually send these emails." (DMPSJ at 11.) In addition, the third parties were not paid to send the emails to promote Cyberheat's websites, rather were paid a "finders fee if, and only if, someone whom the third party had referred to one of Defendant's websites subsequently subscribes to the website." (Id.) Defendant further argues that "the critical point that the Court must understand is that Defendant never expressly, implicitly or otherwise authorized such person to violate the CAN-SPAM." (Id.) Defendant relies on the fact that the Terms and Conditions specifically forbids affiliates to violate the CAN-SPAM Act.

Defendant's express position is that as long as Defendant did not permit or condone the illegal activity, Defendant cannot be held liable under the Act. The egregious emails were sent by third parties who "were not the Defendant or the Defendant's employees, officers, directors or shareholders." (Id. at 13.) Defendant denies that it initiated, induced or procured the violative emails, as defined by the Statute. Defendant denies that it is liable under the "pay or provide" definition. Defendant insinuates that the Statute requires intent for Defendant to be held liable for the acts of the third parties and there is no direct evidence of intent in the record. "Defendant must have intentionally paid or provided compensation to another to send the illegal email or it must have intentionally induced another to do so." (Id. at 19.) Defendant goes on to argue that Plaintiff is applying a strict liability analysis to include Defendant as a violator for third party acts.

Cyberheat treats and describes the affiliates as more like independent contractors, persons who perform services for another person under an express or implied agreement and who are not subject to the other's control or right to control the manner or means of performing the services, than agents, acting

within the scope of authority in the performance of duties which are expressly or impliedly assigned by the principal. There are no facts to suggest that Cyberheat was violating the Act but for the use of the affiliate promotional program. There are also no facts that Cyberheat directed affiliates to promote its website by violating the Statute. Cyberheat did not direct affiliates to utilize the promotional materials in emails and possibly had an informal arrangement that emails would not be used at all.

Cyberheat also raises questions that suggest that due to the infinitesimally small number of affiliates who used violative email messages, the question of knowledge and duty on the part of Cyberheat is particularly relevant. Plaintiff has focused on 12 Cyberheat Webmasters out of upwards of 50,000 affiliates of which only about 10,000 successfully refered subscribers, or 2/100 of one-percent of the registered affiliates utilized email to promote. (SuppResp at 11.) Cyberheat argues that the government's proposed permanent injunction, in light of the facts here, is overbroad and onerous.

The Defendant contends that it cannot be found in violation of the Act because it did not intentionally induce the violative email messages or intentionally induce its affiliates to send the violative email messages. Defendant asserts that it had no control over the actions of its affiliates. Defendant argues that it did not know about or consent to the violations.

4. Control

Cyberheat's ability to control, monitor and supervise affiliates is a fact question. Cyberheat claims to utilize affiliates on an independent basis with no control over methodology other than the Terms and Conditions Agreement. Cyberheat does not monitor or oversee the actions of affiliates other than accounting for business referred to Cyberheat by an affiliates for which they are compensated. Cyberheat does not direct the promotional activities of the

affiliates, yet they do provide promotional materials. Factually, Cyberheat and its affiliates appear distant and removed, other than some nominal support. The terms of the affiliate agreement evince no intent on the part of Cyberheat or any of the affiliates to enter into a principal-agent relationship.

Yet, based on the duty imposed by this Act, if Cyberheat is not a direct violator of the Statute, it may be vicariously liable for the foreseeable violations of its affiliates. The law of agency, in appropriate circumstances, renders a principal vicariously liable for the torts of its agent. *Am. Soc. of Mech. Eng. v. Hydrolevel Corp.,* 456 U.S. 556, 565-66 (1982). A court may apply traditional rules of agency law to a federal statute's civil liability provision when those rules accord with the statute's purpose and when Congress has not indicated otherwise. *Thomas v. Ross & Hardies,* 9 F.Supp.2d 547, 557 (D.Md.1998). For example, Courts have reasoned that because the Lanham Act's purpose of prohibiting unfair competition would go largely unrealized if it absolved principals from the trademark-infringing acts of their agents, and because the Act itself does not disavow such liability, a cause of action under the Lanham Act may lie vicariously against a principal. *See Am. Tel. & Tel. Co. v. Winback & Conserve Program, Inc.,* 42 F.3d 1421, 1437 (3d Cir.1994).

"Agency is the fiduciary relation which results from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act." *Rest. 2d Agen.* § 1. The creation of an agency relationship ultimately turns on the parties' intentions as demonstrated either by express agreement or by inference from their actions. *Fare Deals, Ltd.,* 180 F.Supp.2d at 685 (operator of web site which was advertised on and hyperlinked to allegedly trademark infringing web site could not be held vicariously liable for false designation of origin or dilution; operator provided no support for and had no authority to control allegedly

infringing web site, and lacked knowledge of alleged infringement.) Courts examine three factors in determining whether a principal-agent relationship exists: first, the principal's right to control the alleged agent; second, the alleged agent's duty to act primarily for the benefit of the principal; and, third, the alleged agent's power to alter the legal relations of the principal. *Id.* These factors provide guidance, but "[t]hey are neither exclusive nor conclusive considerations." *Id.* The parties' intent controls, and a court must ascertain their intent "within the context of the entire circumstances of the transaction or relations." *Id.* The question of agency is a factual matter, and, if any legally sufficient evidence of an agency relationship is produced, it must be submitted to the fact-finder. *Id.* The substance of the parties' relationship, not the label they give it, determines the existence of agency. *Cerniglia v. Pretty,* 674 F.Supp. 1167, 1170 (D.Md.1987).

A principal will be held liable for an independent contractor or agent's wrongdoing "upon matters which the principal might reasonably expect would be the subject of representations, provided the other party has no notice that the representations are unauthorized." *Rest. 2d Agen.* §258. Vicarious liability is indirect legal responsibility. It is the attribution of a wrongdoer's actions to an innocent third party by virtue of their relationship. Under common–law tort rules, a joint tortfeasor may bear vicarious liability for the violations of others. Joint tortfeasors are those either in apparent or actual partnership, or with authority to bind each other in transactions with third parties, or with the ability to exercise joint ownership or control over the violator. 57B *Am. Jur.2d Negligence* §1096; *see Hard Rock Café*, 955 F.2d at 1149; *see also Rest.2d Agen.* §§ 261, 262.

In finding vicarious liability, too, the relationship between the defendant and the alleged violator is very significant. For a parent to be held secondarily

liable for its subsidiary's acts, there must be a sufficient link between them. In *Banff Ltd. v. Limited, Inc.*, 869 F. Supp. 1103 (S.D.N.Y. 1994), a corporate parent was held not vicariously liable for its subsidiary's trademark infringements where the parent made no decisions regarding sales and purchases and had no involvement in operating any of the subsidiary's retail stores, and where the two had different headquarters, kept separate financial records, and filed separate tax returns. In *Am. Tel. & Tel. Co.,* 42 F.3d at 1437, the court held that a telecommunications company, offering users access to the plaintiff's network at discounted prices, would be vicariously liable under the Lanham Act for its sales representatives' overtly stating or misleading customers to believe that its programs were affiliated with the plaintiff if those actions were foreseeable and the customers had no notice that the representations were unauthorized. That court applied basic principal and agent law and concluded that when a principal authorizes its independent contractor or agent to conduct and conclude a transaction with third parties on the principal's own behalf, and the principal benefits financially from the contracts, the principal will be liable, based on the agents' foreseeable infringing actions upon which it would be reasonable for the third party to rely, provided the third party has no notice that the representations are unauthorized. In *Mini Maid Services Co. v. Maid Brigade Systems, Inc.*, 967 F.2d 1516 (11th Cir. 1992), the court held that a franchiser may not be held vicariously liable for one of its franchisees' trademark infringements. Since, it held, the law imposes no duty upon a franchiser to exercise reasonable diligence to prevent independent acts of trademark infringement by franchisees, this defendant was not liable for its franchisees' enjoying the benefits of a yellow pages listing from one of the plaintiff's franchisees after having purchased the phone number from the latter.

A factual question is raised by both parties concerning how much power and ability Cyberheat had to control, monitor or supervise affiliate operations and whether the company acted reasonably under the circumstances.

5. Knowledge

Further of concern is the question of Defendant's alleged knowledge of violations and inaction to stop violations. Defendant contends that it did not know about or consent to the violations.

Notice of the violations to Defendant and whether Defendant's response to the notice of the affiliates' violations was reasonable under the circumstances is a fact question. *See Perfect 10, Inc. v. CCBill, LLC*, 340 F.Supp. 2d 1077 (C.D. Cal. 2004). Under the Statute, Cyberheat as a company that offers sexually explicit materials to consenting adults over the Internet, by using affiliates to promote and bring in business. Cyberheat provided sexually explicit materials to affiliates to promote its website. Foreseeably, affiliates could violate the Statute and Rule by utilizing email with sexually explicit materials to promote the website. The Terms and Conditions Agreement appears to sufficiently warn the affiliates of what Cyberheat will and will not tolerate.

Although, Plaintiff's investigation reflects that Cyberheat received information that the affiliates were violating the Statute and then did not follow their own promise to terminate violating affiliates. The examples resulting from Plaintiff's investigation are, as follows: Affiliate 28487 who sent four unsolicited violative commercial email messages in August 2004, but not terminated until October 2005; Affiliate 28426 who sent one unsolicited violative commercial email message in August 2004, but has never been terminated; Affiliate 11604 who sent 45 violative messages in August 2004 and has not been terminated; Affiliate 36828 who sent 26 violative messages and is an active account; Affiliate 26377 who sent 1 unsolicited message and is still an active

account; Affiliate 38485 who sent 4 messages and is an active account; Affiliate 43717 who sent five unsolicited messages and is still an active account; and, the list goes on. According to Plaintiff, Cyberheat has a pattern of receiving complaints of violative emails, but not responding at all or belatedly responding, then possibly reinstituting violating affiliates. Plaintiff claims that Defendant turned a blind eye to violating affiliates even after they were made aware of the violations. Defendants claim that they acted properly and promptly, under the circumstances.

Generally, whether the breach or violation of a statute has occurred, and whether that breach or violation was without valid excuse is a question of fact for a jury. 65A *C.J.S. Negligence* §842 (2006). Where conflicting evidence is introduced as to any one of the elements necessary to constitute the violation of a statute, a jury question is created, such that it is within the jury's province to assess the credibility of witnesses and determine whose testimony and evidence warrants belief. *Id.; see America Online, Inc. v. National Health Care Discount, Inc.*, 174 F.Supp. 2d 890 (N.D. Iowa 2001).

CONCLUSION

Here, overall, the evidence produced by both parties raises material questions of fact regarding the relationship between Cyberheat and its affiliates. These material questions of fact go to the heart of the relationship between Cyberheat and its affiliates, specifically what if any control or supervision Cyberheat exerted or could or should have exerted over affiliates based on the content of the promotional materials provided. The material questions of fact also go to the knowledge Cyberheat acquired that affiliate violations were occurring, as well as what actions Cyberheat took upon receiving knowledge of violations and whether its actions were reasonable under the circumstances.

Plaintiff argues that these questions involve undisputed facts, but that is not the case, because the evidence is circumstantial, disputed and requires credibility assessments. Reasonable jurors could differ over whether or not Defendant was knowingly procuring or should have known or was consciously avoiding knowing that affiliates were violating the Statute to promote Defendant's website. Plaintiff's evidence concerning Cyberheat's relationship with affiliates is circumstantial and requires the Court to draw factual inferences and make credibility determinations that preclude resolution by summary judgment. Defendant has raised more than some metaphysical doubt as to the material facts. *Matsushita Elec. Indus. Co.*, 475 U.S. at 586. The court recognizes its obligation to view all facts in a light most favorable to the non-moving party and finds that a reasonable trier of fact could differ over whether or not that the relationship between Cyberheat and its affiliates resulted in vicarious liability for violations of the Statute.

A trier of fact may consider the complaints about the affiliates' violative activities to the company and Cyberheat's response to those complaints in reaching a conclusion. These particular facts may result in civil penalties of up to $11,000 per violative email. *Tull v. United States*, 481 U.S. 412 (1987).

Accordingly,

IT IS ORDERED that Plaintiff's Motion for Summary Judgment (Doc. No. 24) and Defendant's Motion for Partial Summary Judgment (Doc. No. 28) are DENIED.

IT IS FURTHER ORDERED that the parties should submit a joint proposed pretrial order on April 27, 2007. A pretrial conference will be set upon receipt of the pretrial order and a trial date will be set at the pretrial conference.

DATED this 2nd day of March, 2007.

David C. Bury
United States District Judge