

(Cite as: 10 NO. 11 J. Internet L. 3)

Journal of Internet Law

May, 2007

Edited by DLA Piper Rudnick Gray Cary

*3 HOW WELL DO YOU KNOW YOUR INTERNET MARKETING PARTNERS?

Tom Hughes [FN1]

Copyright © 2007 by Aspen Publishers, Inc.; Tom Hughes

Finding new and creative ways to reach customers often requires sellers to go outside their established network of affiliates and partners, and do business with lesser-known and perhaps untested companies. While many of these marketers will prove themselves worthy, others may lack expertise or interest in legal compliance, potentially exposing the seller to substantial legal risk. This is especially true today, as enforcement actions against high-profile companies, such as DirecTV, Cingular, and Priceline.com, illustrate that the Federal Trade Commission (FTC) and state Attorneys General (AGs) are increasingly taking aim at sellers for the alleged misconduct of their marketing partners. Unless companies conduct reasonable due diligence on potential partners, they could find themselves facing liability for their partners' actions, and the FTC and state AGs will use their enforcement authority to require such due diligence with respect to future partners.

UNITED STATES V. CYBERHEAT

The most recent and perhaps most extreme example of an enforcement agency attempting to hold a seller liable for the alleged misconduct of marketing affiliates is *United States v. Cyberheat, Inc.*, where the FTC attempted to impose a near strict liability standard on a seller for the email marketing of independent affiliates. [FN1] Cyberheat operates adult entertainment Web sites, which it markets through affiliates, paying them for successful promotions. These affiliates are not owned or otherwise controlled by Cyberheat. According to the complaint, a number of affiliates promoted Cyberheat's site by sending sexually explicit email that did not comply with CAN SPAM's [FN2] warning label requirements. [FN3] As a result, the FTC, through the Department of Justice, filed suit against Cyberheat as an "initiator, sender, and/or procurer" of these allegedly violative emails.

The FTC moved for summary judgment, arguing that, based on the undisputed material facts, Cyberheat should be liable for the acts of its affiliates. According to the court, the primary document in support of the FTC's case was a declaration by an FTC investigator that purported to "show conclusively that Cyberheat and the affiliates were connected, as well as Cyberheat's knowledge of its affiliates activities." [FN4] This included facts showing that Cyberheat:

1. Had affiliates that promoted its Web site by sending sexually explicit email;
2. Had compensated affiliates for referring customers who subscribed to its Web site;
3. Had an inadequate screening process for affiliates;
4. Had not asked affiliates if they planned to use email to promote its Web site;
5. Had received, in the course of one year, some 400 complaints from consumers that received unwanted SPAM;
6. Had not terminated every affiliate that was the subject of a spam-related complaint and, in some cases, had reinstated affiliates that had been terminated for using spam;
7. Had terms and conditions providing that the affiliates should not use mass, unsolicited email, but did not monitor whether the affiliates had used email marketing, and;

(Cite as: 10 NO. 11 J. Internet L. 3)

8. Had provided free Web hosting and promotional tools that gave affiliates the power to put hyperlinks to explicit promotional materials in their emails. [FN5]

According to the FTC, these facts established 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." [FN6] Intent or knowledge was irrelevant, according to the FTC:

What is required to find Cyberheat liable under the Act is something less than 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. [FN7]

The FTC thus asked the court to impose a "strict liability-lite" standard on sellers for the conduct of their affiliates, which the court refused to do. Rather, the court found that "control over the affiliates and knowledge of the violations of the affiliates are two issues that are pivotal." [FN8] It then went on to find that knowledge of *4 violations and any actions, or lack thereof, to stop them was a question of fact, as was Cyberheat's ability to control the affiliates. According to the court:

These material questions of fact go to the heart of the relationship between Cyberheat and its affiliates. Specifically, the main question at hand is 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. [FN9]

While the court did not clearly articulate a standard, the decision, especially the above quote, indicates that it will, at a minimum, require constructive knowledge, that is, some control or ability to control the affiliates responsible for the violations. The FTC may ultimately establish the requisite elements, but at least Cyberheat has the ability to defend itself, rather than be liable for anything beyond accidental violations.

While the FTC was unable to impose strict liability-lite in this case, its efforts in this regard cannot be ignored. The FTC found it significant that Cyberheat had provided Web hosting, technical support, site statistics, and a URL linking to its site, all of which can be used for legitimate Web-based referral marketing. Yet, the FTC asserted that Cyberheat should be liable for any misuse because these tools could be used for illegal spam. The FTC's logic is troubling because most any tool for legitimate marketing could be used deceptively.

SPYWARE AND THE FALLOUT FROM DIRECTREVENUE

If Cyberheat left any question about the FTC's intention to hold sellers liable for the conduct of their marketing affiliates, Commissioner Jon Leibowitz removed any doubt. In a recent interview with the Washington Post, Commissioner Leibowitz made it clear that the FTC plans to address the problem of spyware by targeting prominent sellers that advertise their products through companies that distribute spyware. The intent, according to Commissioner Leibowitz, is to "stop the demand side of spyware." The FTC's plan is to "send letters to major corporations and entities that place the majority of these ads. This is a wake-up call to put them on notice. That would be a good way to choke off the money." [FN10] For this to be effective, the FTC will necessarily be required to follow these notice letters with enforcement efforts aimed at holding advertisers liable for any allegedly deceptive practices of their affiliates that might employ spyware. In doing so, the FTC will likely seek to hold advertisers to a strict liability-lite standard.

The FTC recently brought an action against spyware distributor DirectRevenue LLC, in which it imposed injunctive relief and forced DirectRevenue to return \$1.5 million. [FN11] The FTC did not, however, target the com-

(Cite as: 10 NO. 11 J. Internet L. 3)

panies that advertised through DirectRevenue. Its decision to target them now might be the result of the NY Attorney General's beating them to the punch.

In January 2007, the NY Attorney General reached ground-breaking settlements with Priceline.com Inc., Travelocity.com LP, and Cingular Wireless LLC for advertising through DirectRevenue. [FN12] According to the Attorney General, DirectRevenue installed adware on consumers' computers without providing adequate notice. Once installed, the adware delivered a stream of advertising, including ads from Priceline, Travelocity, and Cingular. Touting the settlement, the Attorney General explained that advertisers "can no longer insulate themselves from liability by turning a blind eye to how their advertisements are delivered, or by placing ads through intermediaries, such as media buyers." [FN13] Thus, whether or not Priceline, Travelocity, and Cingular intended or knew that their ads were being served via spyware, they were held liable, at least in part, for DirectRevenue's failure to provide consumers with sufficient notice and adequate consent. The resulting Assurance of Discontinuance provides in the findings:

(8) Even though Cingular was aware of controversy surrounding the use of adware and was aware, or should have been aware, of Direct Revenue's deceptive practices, including surreptitious downloads, Cingular continued to use Direct Revenue adware programs to distribute its online advertisements.

...

(11) The OAG finds that, by using Direct Revenue's adware programs to advertise its products and services on the Internet, Cingular has engaged in deceptive business practices [FN14]

Just as the FTC wanted to impose near strict liability on Cyberheat because it was possible that its service could be advertised by email that violates the CAN-SPAM Act, the NY Attorney General premised liability, at least in part, because companies should have known about the "controversy surrounding the use of adware."

CASES IN WHICH THE FTC IMPOSED A DUE DILIGENCE REQUIREMENT

Requiring due diligence prior to using affiliates has been a favored remedy sought by the FTC in cases when *5 sellers were held liable for the conduct of their affiliates. In December 2005, the FTC reached a stipulated judgment and order with DirecTV, in part for its affiliates' violations of the national Do-Not-Call (DNC) registry. According to Commission Chairman Deborah Platt Majoras, the "multimillion dollar penalty drives home a simple point: Sellers are on the hook for calls placed on their behalf." [FN15] While the \$5.3 million penalties (the largest to date for DNC violations) received most of the publicity, the consent order's injunctive provisions are far more significant. These include requiring that DirecTV:

1. conduct due diligence on those persons it authorizes to engage in telemarketing on its behalf. This includes making certain that the telemarketer has in place and enforces procedures for preventing violations of the DNC and call abandonment provisions of the Telemarketing Sales Rule.
2. monitor the telemarketing campaigns of its telemarketers to ensure compliance with the DNC and call abandonment provisions of the Telemarketing Sales Rule. [FN16]

In another case, the FTC imposed due diligence requirements on CompUSA. This resulted from a manufacturer of computer equipment, Q.P.S. Inc., failing to honor its rebates, which CompUSA had advertised. According to the FTC, thousands of Q.P.S. products were sold with rebates that were not paid in a timely manner. The overdue rebates ranged from \$15 to \$100 and many consumers received their rebates one to six months after the due-date, or never at all. As a result, the FTC charged CompUSA with engaging in unfair and deceptive advertising practices relating to rebate offers, in part because the Q.P.S. rebates were not paid by their respective due dates. [FN17]

The consent order reflects the FTC's belief that CompUSA had a responsibility to check the ability of Q.P.S. to pay these rebates before CompUSA advertised them in its stores. The FTC's consent order not only required Com-

(Cite as: 10 NO. 11 J. Internet L. 3)

pUSA to pay all valid Q.P.S. rebates that were left unpaid but also placed due diligence requirements on CompUSA before offering rebates from manufacturers in the future. The terms of the order state that CompUSA is prohibited from advertising manufacturers' rebates unless:

1. it has an established record with the manufacturer demonstrating that the manufacturer has consistently paid rebates in a timely manner; or
2. if it does not have such an established record with the manufacturer, CompUSA has conducted a reasonable financial analysis of the manufacturer that demonstrates the manufacturer's ability to pay the offered rebate. [FN18]

CONCLUSION

There is no question that the FTC and state enforcers will continue their efforts to hold sellers liable for the conduct of their affiliates. As the Cyberheat case demonstrates, they will likely try to impose a strict liability-lite standard, holding sellers liable for the conduct of their affiliates, whether the seller knew or consciously avoided knowing about the conduct. This is especially likely in areas involving email, Internet advertising, and other areas that are more closely regulated and are of particular interest to the FTC. To avoid potential liability, sellers should:

- Screen affiliates on the front end using well developed criteria and following them. If an affiliate does not meet the criteria, no matter how much revenue it says it will deliver, sellers should not accept that affiliate.
- Clearly state terms and conditions indicating what the affiliate may do and what the affiliate may not do. For example, if the affiliate is authorized to provide a link to a product or service via a banner ad or hyperlink, state that and also mention that the affiliate may not engage in mass mailing, telemarketing, email marketing, or other form of marketing. Also, include a provision stating that the seller can terminate the affiliate for cause.
- If the affiliate is using novel technology that relies on consumer consent, require in the terms and conditions of the agreement that the affiliate obtain express verifiable consent. Also, have the affiliate explain and demonstrate how the technology will work and how it will obtain consent.
- Routinely monitor the conduct of affiliates to make sure they are complying with the applicable laws and the terms and conditions of the arrangement.
- Have clearly defined procedures for monitoring and, where appropriate, investigating complaints.
- Terminate affiliates that violate the law, terms, and conditions, or are responsible for a significant number of complaints.

In the end, sellers have a choice: Act as though strict liability is the standard, or be prepared to litigate the issue should the FTC conduct an investigation. This is especially true for those sellers that market through channels such as email and telemarketing, which are highly regulated and have the attention of enforcement agencies. Compliance is usually cheaper than litigation.

[FN1]. Tom Hughes is a partner at the law firm of Hunton & Williams specializing in advertising and consumer law. Prior to joining Hunton & Williams, he was a staff attorney at the Federal Trade Commission. He blogs about developments in advertising and consumer law at www.reasonablebasis.com.

[FN1]. *United States v. Cyberheat, Inc.*, No. CV-05-457, 2007 U.S. Dist. LEXIS 15448, at *1 (D. Ariz. Mar. 2, 2007).

[FN2]. Controlling the Assault of Non-Solicited Pornography And Marketing Act, 15 U.S.C. 1-157 §§ 1-16 (2003).

[FN3]. *Cyberheat, Inc.*, U.S. Dist. LEXIS 15448, at *29-30.

[FN4]. *Id.* at *25.

(Cite as: 10 NO. 11 J. Internet L. 3)

[FN5]. Id. at *29.

[FN6]. Id. at *30.

[FN7]. Id. at *31 (quoting Commission's Memorandum in Support of Motion for Summary Judgment at X (emphasis added)).

[FN8]. Id. at *19.

[FN9]. Id. at *46.

[FN10]. Cindy Skrzycki, "Stopping Spyware at the Source," Washington Post, Mar. 6, 2007, at D1.

[FN11]. In reDirectRevenue, LLC, No. 052-3131, at 6, 9 (FTC Feb. 16, 2007) (agreement containing consent order), available at <http://www.ftc.gov/os/caselist/0523131/index.htm> (follow relevant hyperlink).

[FN12]. In re Priceline.com, Inc., at 2-3 (NY Att'y Gen. Internet Bureau Oct. 23, 2006) (assurance of discontinuance); In re Travelocity.com, LP, at 2- 3 (Dec. 18, 2006); In re Cingular Wireless, LLC, at 3 (Jan. 29, 2007), available at http://www.oag.state.ny.us/press/2007/jan/jan29b_07.html (follow "Assurance of Discontinuance" hyperlink at bottom of press release).

[FN13]. Press Release, "NY Att'y Gen., Groundbreaking Settlements Hold Online Advertisers Responsible for Displaying Ads Through Deceptively Installed 'Adware' Programs" (Jan. 29, 2007), available at http://www.oag.state.ny.us/press/2007/jan/jan29b_07.html.

[FN14]. In re Cingular Wireless, LLC, at 3 (assurance of discontinuance).

[FN15]. United States v. DirecTV, Inc., No. 05-1211 (C.D. Cal. Dec. 13, 2005) (stipulated judgment and order for permanent injunction against DirecTV, Inc.), available at <http://www.ftc.gov/os/caselist/0423039/0423039.htm> (follow relevant hyperlink).

[FN16]. Id. at ¶¶ IIA & D.

[FN17]. In re CompUSA, Inc., No. 022-3278 (FTC Mar. 11, 2005) (complaint), available at <http://www.ftc.gov/os/caselist/0223278/0223278compusa.htm> (follow relevant hyperlink).

[FN18]. Id. at 3-4 (agreement containing consent order), available at <http://www.ftc.gov/os/caselist/0223278/0223278compusa.htm> (follow relevant hyperlink).

END OF DOCUMENT