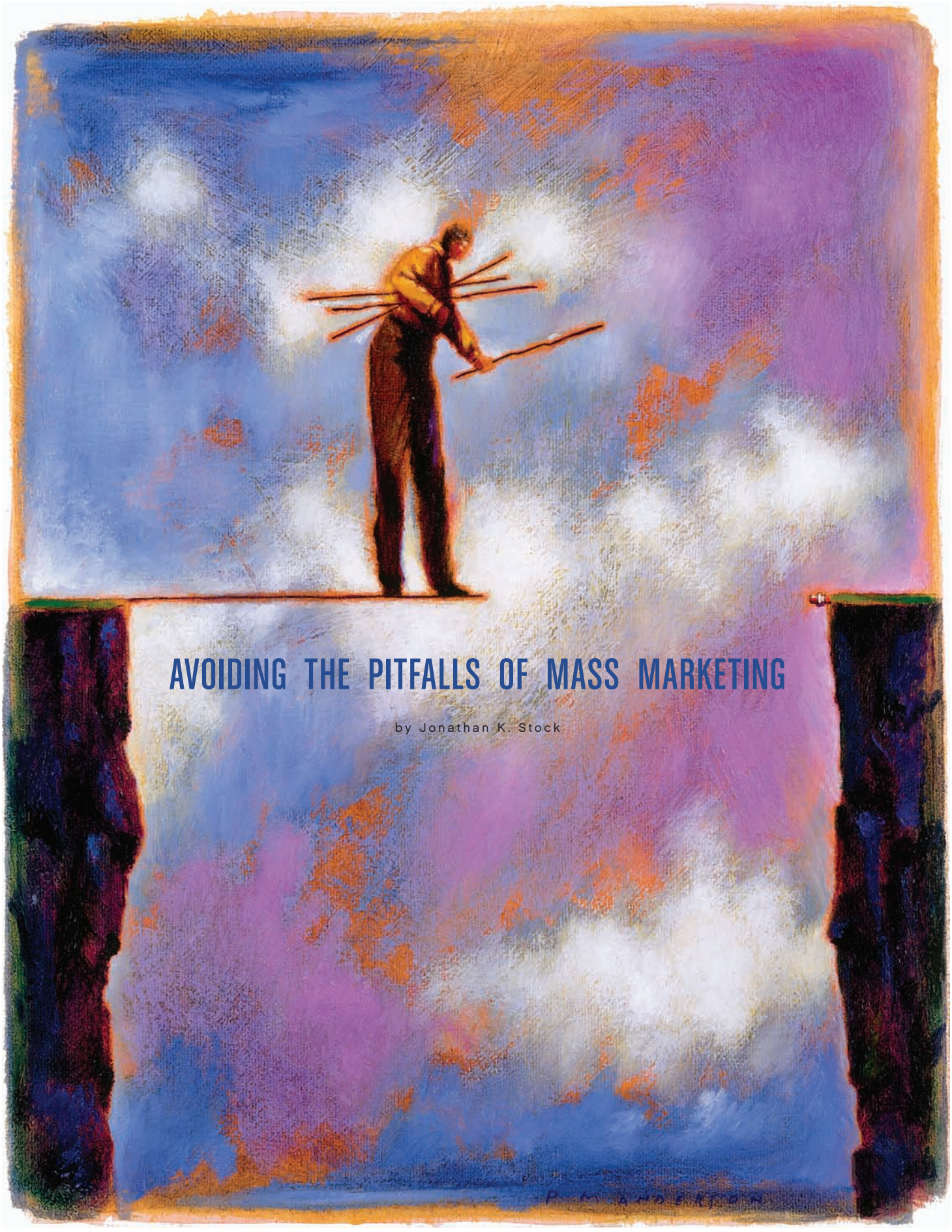

AVOIDING THE PITFALLS OF MASS MARKETING

by Jonathan K. Stock

o matter how great a company's product or service, promoting that product or service to customers can be essential. Many businesses depend upon mass marketing to achieve this objective. Often, unbeknownst to those businesses, the mass-marketing campaigns performed on their behalf ignore federal laws and regulations.

While it may be tempting to leave advertising decisions to an advertising agency or in-house marketing department, the pitfalls from a mistake in mass marketing have become increasingly apparent. An advertising campaign that violates one of the myriad laws and regulations governing mass marketing can turn a single bad decision into literally thousands of statutory violations. Those violations can threaten crippling liability when harnessed to a class action seeking statutory damages or subjected to an enforcement action by a federal agency. To avoid those mistakes, it is critical for businesses to understand and seek guidance on the laws governing mass marketing before they simply sign off on the next advertising campaign.

Over the past several decades, mass marketing has undergone a revolution driven by technology. The old methods of mass marketing (*i.e.*, mail, newspaper advertisements, signage, and in-person solicitation, etc.) are still available but have been increasingly pushed aside. Newer methods (*i.e.*, email, faxing, and telemarketing) have gained in prominence. These newer methods are often more attractive to businesses because they reach more customers at a reduced cost.

Congress has tried to keep pace with these changes in technology by imposing limits on mass marketing. Federal laws now govern commercial advertisements sent via email, fax, and telephone. The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7701 *et seq.*) regulates the transmission of commercial email. The TCPA (Telephone Consumer Protection Act, 47 U.S.C. § 227) does the same for commercial fax advertising and telemarketing. For telemarketing, the Federal Trade Commission ("FTC") has also played an important role, by adopting the TSR (Telemarketing Sales Rule, 16 C.F.R. § 310), which is the regulation that enforces the Do Not Call Registry. Complying with these federal laws and regulations is essential for any mass marketer.

COMPLYING WITH THE TCPA FOR FAXING

Faxing is a common method of business-to-business communication that initially had some appeal for mass marketing. That appeal, however, waned considerably when plaintiffs began enforcing the TCPA. The TCPA makes it unlawful for any person "to use any telephone facsimile machine, computer, or other device to send, to a telephone facsimile machine, an unsolicited advertisement." 47 U.S.C. § 227(b)(1)(C). An important exception to this rule occurs if the sender has "an established business relationship with the recipient," obtained the recipient's fax number in an appropriate and voluntary fashion, and provided the recipient with the opt-out notice required by the Act. *Id*. at §§ 227(b)(1)(C) and (b)(2)(D).

For faxes that do not qualify for the exception, the TCPA imposes a broad ban on unsolicited advertisements. An unsolicited advertisement includes "any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person's prior express invitation or permission, in writing or otherwise." *Id*. at § 227(a)(5). Thus, the burden is on the fax sender to have the recipient's "prior express invitation or permission" before sending a fax.

What it means to have the recipient's "prior express invitation or permission" to send a fax has long been the subject of considerable debate. Written permission, though not required, provides a clear and well-documented expression of consent, but it is often impractical for businesses to obtain it. The Federal Communications Commission ("FCC") has offered further guidance on how to obtain a customer's prior express invitation or permission:

> In the absence of an EBR [established business relationship], the sender must obtain the prior express invitation or permission from the consumer before sending the facsimile advertisement. Prior express invitation or permission may be given by oral or written means, including electronic methods. We expect that written permission will take many forms, including e-mail, facsimile, and internet form. Whether given orally or in writing, prior express invitation or permission must be express, must be given prior to the sending of any facsimile advertisements, and must include the facsimile number to which such advertisements may be sent. It cannot be in the form of a "negative option" [*i.e.*, a fax asking the recipient to call and request not to receive any further faxes]. However, a company that requests a fax number on an application form could include a clear statement indicating that, by providing such fax number, the individual or business agrees to receive facsimile advertisements from that company or organization.

See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Junk Fax Prevention Act of 2005, CG Docket Nos. 02-278 and 05-338, FCC 06-42 (released Apr. 5, 2006) (Report and Order) at ¶ 45. Because any form of permission obtained by a fax sender may later be challenged in court, the sender should document the express permission that it received and follow policies and practices for fax advertising that are consistent with the customer's consent.

As noted above, the established business relationship is a critical exception to the statute's requirement for fax senders to have the recipient's express invitation or permission to send faxes. The importance of the exception is reflected in the TCPA's history of enforcement. For mass marketing conducted prior to the 2005 amendment, businesses were sometimes being sued for sending faxes to their own customers. To put a stop to this abusive practice, Congress amended the TCPA in 2005 to confirm that the TCPA permits fax senders to send faxes to recipients with whom they have an established business relationship. The FCC defines "established business relationship" as "a prior or existing relationship formed by a voluntary two-way communication between a person or entity and a business or residential subscriber with or without an exchange of consideration, on the basis of an inquiry, application, purchase or transaction" regarding the advertiser's products or services as long as the "relationship has not been previously terminated by either party." *Id.* at ¶ 18. This is ultimately good news for mass marketers because "a sender that has an EBR with a customer may send a facsimile advertisement to that customer without obtaining separate permission from him." *Id.* at ¶ 45.

The enforcement of the TCPA has both a public and private component. Actions can be brought by the FCC, state attorneys general, or private individuals. Enforcement actions by private individuals can seek injunctive relief and an award of $500 per unsolicited fax (or up to $1,500 if the defendant "willfully or knowingly" violated the Act). 47 U.S.C. § 227(b)(3). Actions by state attorneys general can seek the same relief on behalf of the state's residents. *Id.* at § 227(f)(1). The FCC may also assess a forfeiture of up to $11,000 for each violation of the TCPA.

The FCC remains an active enforcer of the TCPA, and a list of its recent enforcement actions appears on its web site. In a Forfeiture Order issued last March, the FCC fined The Hot Lead Company $2,591,500 for "willful or repeated violations" of the TCPA "by delivering at least 417 unsolicited advertisements to the telephone facsimile machines of at least 149 consumers." *See In re The Hot Lead LLC d/b/a The Hot Lead Company*, File No. EB 06-TC-120 (Forfeiture Order, adopted Mar. 14, 2008).

Individual fax recipients have also filed class actions seeking millions of dollars in damages for fax advertising campaigns that have supposedly gone awry. A list identifying several hundred of those TCPA class actions can be found at http://www.tcpalaw.com/free/cases.htm.[1] While very few TCPA class actions have gone to trial, a number have resulted in significant settlements. Two examples of those settlements over the past year are *Mey v. Herbalife International, Inc. et al.*, Case No. 01-C-263 (Cir. Court of Ohio Cty., W. Va.), a TCPA class action settled for $7 million, and *Derose Corp. v. Goyke Health Center, P.C.*, Case No. 06 CH 6681 (Circuit Court of Cook Cty., Ill.), an Illinois TCPA case styled as a class action settled from insurance proceeds for $4 million.

What is particularly ironic about the wave of TCPA class actions is that the TCPA's statutory-damage award was originally intended to permit individual plaintiffs to recover

damages without being represented by counsel. As former Senator Fritz Hollings (D-SC), the TCPA's sponsor, explained, "Small claims court or a similar court would allow the consumer to appear before the court without an attorney. The amount of damages in this legislation [$500 per violation] is set to be fair to both the consumer and the telemarketer." 137 Cong. Rec. S16205 (Nov. 7, 1991); *see also* 41 U.S.C. § 227(b)(3)(B). Those individual cases now play a relatively small role in private enforcement.

The trend toward filing TCPA class actions began with the decision issued in *Nicholson v. Hooters of Augusta*, Case No. 95-RCCV-616 (Ga. Sup. Ct. Apr. 25, 2001), which awarded just under $12 million in damages to 1,321 class members who each received six unsolicited fax advertisements. Since then, a small cottage industry has developed that has been supported by TCPA plaintiffs who have filed class actions against some of America's best-known companies, including Wal-Mart and the Dallas Cowboys.

What makes these suits dangerous is the toxic combination of statutory damages (assessing $500 per violation, or up to $1,500 if the violation is willful) and the large numbers of fax advertisements typically sent in a mass-marketing campaign. Highlighting this point, one suit filed against a fax broadcaster sought an eye-opening $2.2 trillion in damages. *Kirsch v. Fax.com, Inc.*, Case No. CV810516 (Santa Clara Cty. Cal. Super.) (filed Aug. 22, 2002). While Congress in 2005 stepped in to amend the TCPA and make clear that businesses are allowed to send faxes to customers with whom they have an established business relationship, plaintiffs have continued to file TCPA class actions, and businesses engaged in mass marketing should remain wary.

COMPLYING WITH THE TCPA AND TSR FOR TELEMARKETING

The principal restrictions on telemarketing come from the TCPA and the Telemarketing Sales Rule, or TSR. The TCPA prohibits certain telemarketing practices, including:

(1) The use of an automatic dialing system or prerecorded voice to make sales calls to emergency phone lines, medical offices, hospital rooms, homes for the elderly, paging services, or cellular phones. 47 U.S.C. § 227(b)(1)(A)(i)–(iii);

(2) The use of artificial or prerecorded voice telemarketing, except where there is an emergency or the call recipient gives prior consent. 47 U.S.C. § 227(b)(1)(B); and

(3) The use of an automatic dialing system that occupies two or more telephone lines of a single business simultaneously. 47 U.S.C. § 227(b)(1)(D).

In addition, the FCC requires a person or entity placing telemarketing calls to keep a record of residential phone numbers for all persons who have asked not to receive further telemarketing calls from that person or entity. That record must be maintained for at least five years.

The TCPA provides the same menu of enforcement options for telemarketing violations as for unsolicited fax advertising. It creates a private right of action for individuals to seek injunctive relief or damages in court of up to $500 per violation, or $1,500 if the telemarketer "knowingly" or "willfully" violated the Act. 47 U.S.C. § 227(b)(3). Enforcement actions seeking the same relief can also be brought by state attorneys general. *See* 47 U.S.C. § 227(f)(1). Likewise, the FCC may assess penalties of up to $11,000 per violation against parties that violate the TCPA.

The TSR is best known as the regulation enforcing the Do Not Call ("DNC") Registry. It was promulgated by the FTC under the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. §§ 6101–6108). 16 C.F.R. § 310.4(b)(iii)(B). The DNC Registry is a list of telephone numbers to which unsolicited telemarketing calls are generally prohibited. *Id.* The DNC Registry has grown from its inception to include more than 145 million telephone numbers. *See* "Notice of Proposed Rulemaking" by FCC at 3 (released Dec. 4, 2007).

There are a few important exceptions that permit calls to numbers on the DNC Registry. The DNC Registry does not prohibit calls to persons with whom the seller has an established business relationship. 16 C.F.R. § 310.4(b)(iii)(B)(ii). In addition, telemarketing calls are permitted to persons who register their telephone numbers with the DNC Registry but have nonetheless provided the seller with their express written consent to be contacted. 16 C.F.R. § 310.4(b)(iii)(B)(i). In most instances, calls to businesses are also exempt from the TSR's regulations. 16 C.F.R. § 310.6(b)(7). There is also a safe harbor if a call is inadvertently made to a number on the DNC

Registry, as long as the telemarketer can show that it otherwise routinely complies with the TSR.[2]

In addition to the Registry, the TSR includes other noteworthy restrictions. Telemarketers must disclose upfront the name of the seller and the fact that the call is being made for sales purposes. For a transaction, telemarketers must disclose the total amount of the sale, any restrictions on the sale, and whether there is a refund policy. Additional disclosures are required for sweepstakes telemarketing, including the fact that no purchase is necessary in order to participate, the odds of winning, and any cost associated with participation. Telemarketing should not be conducted before 8 a.m. or after 9 p.m. in the recipient's time zone. Telemarketers must obtain "express verifiable authorization" before engaging in certain transactions, such as taking a draft directly from a bank account. Telemarketers must also maintain certain records related to their activities.

The consequences of violating the TSR are significant. A violator can be subject to fines of up to $11,000 per telemarketing call in violation of the rule and can be enjoined from committing further violations.[3] In addition to regulatory actions, the TSR authorizes enforcement actions by state attorneys general and private individuals.[4]

Businesses that engage in telemarketing should keep in mind that telemarketing restrictions are not uniform. Many states have independent state laws regulating telemarketing or maintain their own do-not-call lists. The TSR makes clear that those state laws are not preempted.[5] Likewise, the TCPA does not generally preempt state laws, but instead expressly permits state laws that "impose[] more restrictive intrastate requirements." 47 U.S.C. § 227(e)(1). As a result, state laws can and do impose additional and overlapping restrictions on telemarketing and fax advertising.

COMPLYING WITH THE CAN-SPAM ACT FOR EMAIL

Before the CAN-SPAM Act, the rapid expansion of email marketing resulted in a host of overlapping and conflicting state-law restrictions. State governments passed laws in an effort to stem the tide of billions of spam emails that cost recipients in time, productivity, resources, and equipment. Every year, businesses and consumers spend considerable resources on anti-spam software alone. According to recent estimates,

An advertising campaign that violates one of the myriad laws and regulations governing mass marketing can turn a single bad decision into literally thousands of statutory violations.

more than 180 billion emails are sent every day, and spam email now accounts for up to 95 percent of all email transmitted. *See* "Email and webmail statistics," by Mark Brownlow (Apr. 2008) (http://www.email-marketing-reports.com/metrics/email-statistics.htm) (a study by The Radicati Group from October 2006 estimated the number of emails sent per day in 2006 to be around 183 billion); "Study: 95 percent of all e-mail sent in 2007 was spam," by Matt Asay (Dec. 12, 2007) (http://www.cnet.com/8301-13505_1-9831556-16.html). Against this backdrop, the CAN-SPAM Act has established a uniform standard for commercial email.

The CAN-SPAM Act, which became effective in 2004, preempted a patchwork of preexisting state laws, replacing those laws with a national standard governing commercial email. State laws still play an important role governing false

and deceptive advertising, but the CAN-SPAM Act covers the rest of the spectrum for commercial email. The CAN-SPAM Act regulates the transmission of commercial emails but does not prohibit them. An email qualifies as a commercial email subject to the Act if its "primary purpose" is a commercial advertisement.

The CAN-SPAM Act prohibits a sender of commercial email from using false information and deceptive subject lines. In each email, senders must include a "from" line that accurately identifies the sender of the email, along with a valid physical postal address. Moreover, they may not use another person's email or computer account to send commercial email. Senders must also clearly and conspicuously identify unsolicited commercial email as advertisements or solicitations, and they must include a warning label on unsolicited commercial email containing sexually oriented material. Each commercial email must also contain a clear and conspicuous notice to recipients of their opportunity to unsubscribe from future mailings, using a method that will remain operational for 30 days after the email is sent. The sender must stop sending emails to recipients within 10 business days of receiving the opt-out request. Finally, senders are prohibited from using automated means to harvest email addresses from web sites or online service providers that have policies of not sharing email addresses, and they cannot use automated means to register for multiple email accounts to be used to send spam.

Enforcement of the CAN-SPAM Act includes both a public and a private component. The Act permits enforcement actions by the FTC, state attorneys general, and providers of internet access services, commonly called "ISPs." As with the TCPA, the FTC can levy fines for violations of the CAN-SPAM Act of up to $11,000 per violation.[6] A state attorney general may sue on behalf of the state's residents, seeking an injunction or statutory damages for the actual loss suffered by the state's residents or up to $250 per violation, whichever amount is greater. Damages generally may not exceed $2 million, although that amount may be trebled for a knowing and willful violation. The damages available to ISPs suing under the Act are slightly different. ISPs can sue both the sender of the email and the business advertising its wares (if different from the sender) for up to $25 per violation or, if the header information on the email is false or misleading, up to $100 per violation. Damages are generally capped at $1 million, although a court can treble that amount if the sender knowingly or willfully violated the CAN-SPAM Act. For enforcement actions by either state attorneys general or ISPs, the damage caps are lifted if the header information on the email is false or misleading.

The CAN-SPAM Act's broad definition of "ISP" has left the door open for many businesses, including non-internet-based businesses, to consider enforcement actions. An ISP eligible to sue includes providers of "Internet access services adversely affected by a violation."[7] (An "Internet access service" is "a service that enables users to access content, information, electronic mail, or other services offered over the Internet.") While this definition would certainly include well-known ISPs such as AOL and EarthLink, it could also include businesses that provide internet service to their employees. As one staff attorney for the FTC remarked, businesses providing internet services to employees may qualify as ISPs under the CAN-SPAM Act and therefore have the right to sue email advertisers impinging upon those internet services.[8] If businesses begin to take a more active role in enforcement, the impact could be significant. A single email sent to each employee of a 10,000-employee company could trigger a $1 million violation of the CAN-SPAM Act.

To date, relatively few private lawsuits have been filed under the CAN-SPAM Act. One recent case filed by social networking giant MySpace made headlines when the company obtained a $230 million judgment against "Spam King" Sanford Wallace and his partner, Walter Rines. *See* "MySpace Wins $230 Million From 'Spam King' Wallace," by Stefanie Hoffman, *ChannelWeb* (May 14, 2008) (http://www.crn.com/security/207800154). Yet enforcement actions like the one brought by MySpace are infrequent. This result can be attributed, at least in part, to the CAN-SPAM Act's relatively narrow private right of action. While ISPs have the right to sue, individual email recipients do not. Moreover, the willingness of ISPs to undertake such enforcement is tempered by the difficulty some ISPs have had in collecting judgments. *See* "AOL gives up treasure hunt," by Jay Fitzgerald, *Boston Herald* (July 24, 2007) (discussing the disappearance of a spammer who owed AOL for a $12.8 million judgment). Private enforcement of the CAN-SPAM Act could improve if more businesses realize that they are eligible to sue as ISPs and act to stem the tide of commercial emails violating the Act.

continued on page 32

continued from page 13

Even in this difficult enforcement environment, the FTC has played an important role in pursuing violators of the CAN-SPAM Act and assessing significant fines. In March of this year, for example, online advertiser ValueClick, Inc., agreed to pay a fine of $2.9 million, in part for alleged violations of the CAN-SPAM Act. *See* "ValueClick to Pay $2.9 Million to Settle FTC Charges" (press release dated Mar. 17, 2008) (http://www.ftc.gov/opa/2008/03/vc.shtm). In February, the FTC won an award of $2.6 million in an Illinois federal-court decision against marketer Sili Neutraceuticals for violating the Act. *See FTC v. Sili Neutraceuticals, LLC*, Case No. 07 C 4541 (N.D. Ill.). The number of enforcement actions by the FTC, however, has not kept pace with the nearly unstinting growth of spam email.

If private or public enforcement of the CAN-SPAM Act were stepped up, many businesses that rely upon email advertising would be in for a surprise. Surveys suggest that the majority of businesses that rely on email advertisements are not aware of the CAN-SPAM Act and do not comply with it. *See* "Majority of Email Marketers Not Aware of CAN-Spam Regulations" (June 29, 2007) (http://www.prleap.com/printer/83322).

CONCLUSION

If your business relies upon mass marketing, be prepared before you hire a mass marketer or launch your next advertising campaign. Have the mass marketer inform you of its marketing plan, including the type of media involved, and ask the right questions to ensure that the mass marketer complies with the applicable laws and regulations. Also, review the policies and procedures of in-house marketing departments to make sure they are compliant. Finally, take steps to protect your business. Insurance contracts typically provide coverage for advertising and property damage. In a number of cases, insurance contracts have either indemnified or paid for the defense of mass marketers who have been sued. Thus, it is important to review your insurance policies with an eye toward mass marketing. Although none of these recommendations can make a business immune to the risk of litigation, adopting the best advertising practices can help your business better avoid litigation and limit liability. ■

JONATHAN K. STOCK
1.614.281.3967
jkstock@jonesday.com

This article was prepared with assistance from Kasey T. Ingram, an associate in the Firm's Columbus Office.

[1] All web sites herein were last visited on June 25, 2008.

[2] 16 C.F.R. § 310.4(b)(3) (requiring for safe harbor written procedures, trained personnel, a list of telephone numbers not to contact, an updated version of the DNC Registry not more than 31 days old, and the monitoring and enforcement of compliance).

[3] *See* Federal Trade Commission, "Complying with the Telemarketing Sales Rule" (Jan. 2004) (http://www.ftc.gov/bcp/edu/pubs/business/telemarketing/bus27.shtm); 15 U.S.C. § 6105(b) (authorizing the FTC to enforce violations of the Telemarketing Sales Rule as though they were violations of Section 5 of the FTC Act); *FTC v. Consumer Alliance, Inc.*, 2003 U.S. Dist. LEXIS 17423 (N.D. Ill. 2003) (imposing officer liability for violations of the FTC Act and the TSR Rule).

[4] 16 C.F.R. § 310.07(a).

[5] 16 C.F.R. § 310.07(b).

[6] The CAN-SPAM Act also provides for criminal penalties with respect to certain fraud-related violations. *See* 15 U.S.C. § 7703.

[7] *See* 15 U.S.C. § 7706(g) (authorizing suits by providers of internet access services); 15 U.S.C. § 7702(11) (adopting the definition of "Internet access service" from 47 U.S.C. § 231(e)(4)).

[8] *See* BNA, Inc., "Definition of 'ISP' Under CAN-SPAM Could Permit Legal Actions by Employers," 72 *The United States Law Week* 2696 (May 18, 2004).