

January 2007

SPAM

Commercial E-Mail Advertisers: Know the Rules of the Game

By
Michele A. Shuster

The Federal Trade Commission (“FTC”) has identified combating “spam” as one of its top priorities. Recently, 19 international spam enforcement agencies from 15 countries rolled out an “action plan” for combating spam. The plan calls for increased investigative training, establishment of agency contact points who can respond quickly and effectively to enforcement inquiries, as well as the creation of an international working group on spam enforcement.

As a result, you can anticipate increased enforcement activity by the FTC and state regulators against spam. For that reason, it is important to ensure compliance with all state and federal regulations when sending commercial advertisements over the Internet.

First, the law

The “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003” (“Can Spam Act”) became effective January 1, 2004. It imposes a series of requirements on the use of commercial e-mail messages. In addition, the Act gives the FTC civil and criminal enforcement authority, the state attorneys general civil enforcement authority, and citizens a private right of action.

The Can Spam Act requires:

- Inclusion of a legitimate return e-mail and physical postal address for the sender;
- Inclusion of a functioning opt-out mechanism, with a clear and conspicuous notice of the opportunity to opt-out that must remain active for a minimum of 30 days after sending the emails;
- That advertisers honor any opt-out requests within 10 days of the request being made;
- A clear and conspicuous notice that the message is an advertisement or solicitation in the subject line or content of the email; and
- That any sexually oriented material be clearly identified and be positioned at least “one-click away” from the main e-mail.

The Can Spam Act prohibits:

- Falsifying or disguising a sender’s true identity, such as using a misleading sender address;
- The use of misleading subject lines that mask the true purpose of the email;
- The harvesting of e-mail addresses by either automatic means from an Internet web site or proprietary online electronic addresses by combining names, letters and numbers in numerous permutations;
- Knowingly sending false or misleading information; and
- The use of “open relays” to send email.

Potential liability:

The Can Spam Act implicates not only the individuals actually distributing the spam e-mails, but also extends to companies who use their services. If a company knowingly permits a third-party spammer to act on its behalf, it is subject to prosecution under the Act. Companies or individuals enlisting the services of e-mail distributors need to ensure e-mails being sent on their behalf by distributors are in compliance with the law.

Penalties: Violators of the Can Spam Act can be subject to stiff criminal penalties, which include fines and prison time (up to five years). Civil damages can amount to as much as \$250 per spam e-mail. Aggravated violations can lead to the tripling of civil damages. The Act empowers federal and state authorities, as well as Internet access providers, to institute civil actions against offenders.

Please visit the FTC's website at, www.ftc.gov/spam for more information.