

Client Advisory

December 2003

Spam Not Canned, But Marketers Must Comply With New Federal Law, Beginning New Year's Day

Signed into law by President Bush on December 16, 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") has been much hailed and hyped by its supporters as a means of damming the deluge of unsolicited commercial electronic mail, or "spam," which comprises the majority of e-mail traffic. Yet, instead of "canning" spam, the aptly named federal law confirms that marketers can spam, so long as they follow a few ground rules.

Further confusing marketers and consumers (and their lawyers!) alike, with CAN-SPAM set to become effective on January 1, 2004, several of its requirements remain fuzzy. Nonetheless, if you use e-mail to communicate with customers or potential customers, we urge you to familiarize yourself with the Act and to take whatever measures may be necessary to ensure that commercial e-mails you send in the new year are in compliance.

How Does CAN-SPAM Affect State E-mail Laws?

CAN-SPAM will supplant state laws that expressly regulate e-mail or their attachments, except to the extent those laws prohibit falsity or deception. As such, California's new law is largely preempted. Slated to take effect on January 1, 2004, the California statute is the first "opt-in" law in the United States, requiring marketers to obtain permission prior to sending commercial e-mail.

Does CAN-SPAM Establish A National "Do-Not-E-mail" Registry?

The Act authorizes the Federal Trade Commission ("FTC") to establish, as of October 1, 2004, a national "Do-Not-E-mail" Registry akin to the national Do Not Call Registry. No such "Do-Not-E-mail Registry" is required, however. Rather, CAN-SPAM charges the FTC with providing Congress, by July 1, 2004, a plan and a timetable for a Do-Not-E-mail Registry. FTC officials already have expressed reservations about the effectiveness of such a registry. Unlike telemarketers, most spammers are not legitimate businesses and are already violating a myriad of laws. The concern, therefore, is that those who fill our e-mail systems with unwanted get-rich-quick schemes and pornographic material may choose not to abide by the Do-Not-E-mail Registry.

What Types of E-mail Are Covered?

CAN-SPAM primarily regulates "**commercial electronic mail messages**," *i.e.*, e-mails whose primary purpose (which the FTC is to define by January 1, 2005) is to advertise or promote a product or service. This includes e-mails urging recipients to view content displayed on an Internet website operated for a commercial purpose.

Excluded from the definition of commercial e-mail messages are "**transactional or relationship messages**," or e-mails having a primary purpose of:

- facilitating or confirming a previously agreed upon commercial transaction;
- providing recall, warranty, or safety information regarding a product or service used or purchased by the recipient;

- providing notifications concerning changes to ongoing accounts, subscriptions, or other ongoing commercial relationships;
- providing information directly related to an existing employment relationship or a related benefit plan; or
- delivering goods or services which a recipient is entitled to receive under the terms of a previously agreed upon transaction (*e.g.*, software upgrades).

Such “transactional or relationship messages” are not subject to CAN-SPAM’s disclosure requirements discussed below. They must, however, include accurate and non-misleading header information.

Who Must Comply With CAN-SPAM?

Any individual or entity who sends e-mail messages covered by CAN-SPAM, and those who re-transmit such messages, must adhere to CAN-SPAM’s requirements.

Importantly, businesses may be responsible for e-mails sent on their behalf. CAN-SPAM renders liable companies who know, or should know, that their business is being promoted by e-mails that violate CAN-SPAM’s provisions against false or misleading header information (even if such e-mails are “transactional or relationship messages”), and yet take no action to prevent the unlawful transmission or to report the problem to the FTC.

Further, third party providers of products or services to a business which violates the Act’s prohibition against promoting or allowing promotion of a business through unlawful e-mail, may likewise be held liable if such provider either: (i) owns more than 50 percent of such business, or (ii) has actual knowledge of the promotion of the business via a transmission that violates CAN-SPAM, and receives or expects to receive an economic benefit from the promotion.

What Disclosures Are Required?

Advertisement Label: Each commercial e-mail must contain a clear and conspicuous notice that the message is an advertisement or a solicitation, unless a recipient has expressly consented to its receipt. The Act does not specify the form of such notice.

Opt-Out Notice: Each commercial e-mail must display conspicuously a clear notice which details how, whether through a return e-mail address or another Internet based tool, recipients can request not to receive further messages from the sender. The sender may provide a checklist or menu permitting recipients to select the specific types of messages they do or do not want to receive from the sender, provided that any such list or menu includes an option not to receive any future messages. It is unclear whether this requirement forbids the commonly used technique of requiring users to un-check boxes if they elect not to receive the designated type of mail.

Valid Postal Address: Each commercial e-mail must include a valid physical postal address of the sender.

Opt-Outs

Opt-Out Mechanism Should Be Reliable and Functional For 30 Days: The opt-out mechanism described in each commercial e-mail must be effective for at least 30 days following the original date the e-mail is transmitted. This does not apply if the sender is temporarily unable to receive messages because of a technical problem beyond its control (and the problem is fixed within a reasonable time).

Opt-Out Requests Must Be Acted On Immediately: If a recipient requests not to receive commercial e-mails, the sender or any person acting on behalf of the sender may not, more than 10 business days after receipt of the opt-out request, send or assist another in sending to that recipient any e-mail that falls within the scope of the opt-out request. Once an opt-out request is received from a recipient of a commercial e-mail, it is also unlawful to disclose to any third party such recipient’s e-mail address. These restrictions do not apply, however, if a recipient affirmatively consents to receiving commercial e-mail *subsequent* to opting out.

Deceptive Headers

Include Accurate and Non-Misleading Headers: CAN-SPAM makes it unlawful to send an e-mail with header information (*e.g.*, sender name and e-mail address, domain name, and subject line) that is materially false or misleading, *i.e.*, altered or concealed in a manner that impairs the ability of others to identify, respond to, or locate the sender or to investigate the alleged violation. This includes sending an e-mail with header information that is technically accurate, but which was obtained by false pretenses.

No Deceptive Subject Headings: It is unlawful to send a commercial e-mail if the sender knows (or even if such knowledge may be implied on the basis of objective circumstances) that the message's subject heading is likely to mislead recipients as to the contents or subject matter of the message.

Aggravated Violations

The Act categorizes as an "aggravated violation" sending any commercial e-mail if the sender has knowledge (actual or fairly implied on the basis of objective circumstances) that the recipient's e-mail address was obtained by:

- "address harvesting," *i.e.*, using automated means to cull e-mail addresses, without a consumer's awareness or consent, from a website or other online service which displays a notice (via a Privacy Statement or otherwise) that it will not make available to third parties the e-mail addresses it maintains for purposes of initiating e-mails; or
- "dictionary attacks," *i.e.*, using automated means to generate possible addresses by combining names, letters, or numbers.

Also classified as aggravated violations are:

- using automated means to register for multiple e-mail or on-line user accounts from which to transmit prohibited e-mails; and
- hijacking or other unauthorized use of a computer or network to knowingly re-transmit unlawful commercial e-mail.

Criminal Acts

CAN-SPAM criminalizes:

- use of a computer without authorization to transmit multiple commercial e-mails (*i.e.*, more than 100 in a 24 hour period, more than 1,000 in a month, or more than 10,000 in a year);
- relaying or retransmission of multiple commercial e-mails with the intent to deceive or mislead recipients as to the origin of those messages;
- registering for five or more e-mail or on-line user accounts, or two or more domain names, using false information, and then intentionally sending multiple commercial e-mails from such accounts or domain names;
- materially falsifying header information in multiple commercial e-mails; or
- falsely representing oneself to be the registrant or successor to five or more Internet Protocol addresses and then intentionally sending multiple commercial e-mails from such addresses.
- in the event such an offense is committed, the Act provides for (i) criminal penalties, including up to five (5) years of imprisonment and fines, and/or forfeiture of proceeds obtained from the offense or (ii) goods used or intended to be used to facilitate the commission of the offense.

Adult Content

To inform recipients and to facilitate filtering, CAN-SPAM requires that FTC-regulated marks or notices be placed (in a form to be prescribed by the FTC) in the subject heading of messages that are primarily devoted to sexual matters which depict sexually explicit conduct. The FTC has until April 30, 2004 to prescribe such

marks or notices. CAN-SPAM also limits the type of information that is initially viewable to the recipient of such messages to: (i) the marks and notices and other information required by CAN-SPAM to be included, and (ii) instructions on how to access, or display of a mechanism to access, the sexually oriented material.

What Are The Risks of Violating CAN-SPAM?

CAN-SPAM permits the FTC and other appropriate federal agencies, states, and Internet Service Providers (“ISPs”) to enforce its provisions. No individual right of action is allowed. Available remedies include injunctive relief, actual or statutory damages, and attorneys’ fees. Damages in actions brought by the FTC or states may be up to \$250 per violation, up to \$2 million, and those awards may be tripled if the violations are found to be willful or if the misconduct includes an “aggravated violation.” Statutory damages in cases brought by ISPs may be recovered in amounts ranging from \$25 up to \$100 per violation, up to a total of \$1 million. Imprisonment of up to five years is also available for the criminal violations discussed above.

What Else Should I Know?

The Federal Communications Commission is required to promulgate rules, by September 1, 2004, to protect consumers from the transmission of commercial e-mail transmitted to wireless devices. CAN-SPAM additionally authorizes the FTC to issue regulations implementing the Act and clarifying the meaning of such terms as “commercial electronic mail messages.”

How Might CAN-SPAM Assist Me?

CAN-SPAM could ameliorate the problem of misleading and fraudulent e-mails, assisting consumers as well as legitimate marketers. The creation of a national standard for commercial e-mail should also remedy to some extent the difficulties in both complying with and enforcing the currently numerous and disparate spam-related state laws. As Congress expressed in the Act, however, “The problems associated with the rapid growth and abuse of unsolicited electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well.”

We Can Help

For more information on CAN-SPAM or other issues regarding Internet marketing, e-business, intellectual property or information technology, please contact:

	Direct Dial	Email
Tanya L. Curtis	312.902.5593	tanya.curtis@kmzr.com
D. John Hendrickson	310.788.4495	john.hendrickson@kmzr.com

Published for clients as a source of information about current developments in the law. The material contained herein is not to be construed as legal advice or opinion. © 2003 Katten Muchin Zavis Rosenman. All rights reserved. Katten Muchin Zavis Rosenman is a law partnership including professional corporations.

KMZ Rosenman KATTEN MUCHIN ZAVIS ROSENMAN

www.kmzr.com

525 West Monroe Street
Suite 1600
Chicago, IL 60661-3693
Tel 312.902.5200
Fax 312.902.1061

575 Madison Avenue
New York, NY 10022-2585
Tel 212.940.8800
Fax 212.940.8776

2029 Century Park East
Suite 2600
Los Angeles, CA 90067-3012
Tel 310.788.4400
Fax 310.788.4471

1025 Thomas Jefferson St., N.W.
East Lobby, Suite 700
Washington, DC 20007-5201
Tel 202.625.3500
Fax 202.298.7570

401 South Tryon Street
Suite 2600
Charlotte, NC 28202-1935
Tel 704.444.2000
Fax 704.444.2050

260 Sheridan Avenue
Suite 450
Palo Alto, CA 94306-2047
Tel 650.330.3652
Fax 650.321.4746

One Gateway Center
Suite 2600
Newark, NJ 07102-5397
Tel 973.645.0572
Fax 973.645.0573