



The Spam Spat

How will marketers be affected by the fight against spam?

By Alan L. Friel

THE CONTROLLING THE Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), which became effective on Jan. 1, 2004, represents a congressional response to unsolicited commercial e-mail. (The act is codified at 15 U.S.C. §§ 7701-7713; 18 U.S.C. § 1037; 28 U.S.C. § 994; and 47 U.S.C. 227.) The new law imposes guidelines for regulating certain types of Internet spamming, but does not attempt to outlaw unsolicited e-mailing altogether.

Many, including the National Association of Attorneys General, have criticized the law for not going far enough and for being difficult to enforce. Some critics claim the act will actually cause an increase in spamming and have dubbed it the "You CAN-SPAM Act." One of the act's most vocal supporters is the Direct Marketing Association: The DMA came out strongly against more stringent California legislation, which, along with other state laws, will largely be superseded by CAN-SPAM.

Congress directed the Federal Trade Commission (FTC) to consider various radical measures, including creating a "do-not-e-mail registry," in enforcing the new law. Although the FTC has recommended against such a registry for now, last September it outlined guidelines for a system that would reward informants of CAN-SPAM Act violations with a substantial portion of any civil penalties collected from the spammer. The FTC has until June 16, 2005 to submit a plan for requiring commercial e-mail to be identifiable (such as placing "Adv" or "Advertisement" in its subject line) or to explain why it would recommend against such a plan.

Businesses using e-mail for commercial purposes cannot afford to ignore the CAN-SPAM Act. Although only the most egregious violations will be prosecuted initially, the public outcry against spam can only widen the enforcement net. Every company that directly or indirectly uses commercial e-mail

must bring its activities into compliance with the new law to avoid lawsuits or enforcement actions.

Commercial E-Mails

The CAN-SPAM Act covers any electronic mail "the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," and which is a "commercial electronic mail message" or a "transactional or relationship message." However, it is commercial e-mails that are more heavily regulated.

Portions of the act also deal with potentially fraudulent e-mail involving transactional or relationship messages. So, CAN-SPAM is likely to be relevant for all U.S. businesses that use e-mail to interact with current and prospective customers or affiliates, even if their e-mails are within one of the excepted categories.

The activities regulated under the CAN-SPAM Act fall into seven categories.

Opt-out requirements. The CAN-SPAM Act requires that all commercial e-mails provide a functional "reply to" address or other clearly displayed Internet mechanism that allows the recipient to opt out of future e-mails in a manner clearly and conspicuously specified in the message. Barring unforeseen technical difficulties, this mechanism must remain operational for at least 30 days after transmission of the first message to an individual. The opt-out need not be absolute, and it's permissible to set up a system that gives the recipient the choice to receive only certain kinds of e-mail. It's illegal to send commercial e-mail to someone who has opted out or to transfer or release the e-mail addresses of those who have opted out. Initially, there is a 10-business day grace period to give businesses a chance to update their mailing lists after a person opts out, but the FTC may alter this limit.

For many businesses, it may be worth trying to get an affirmative consent from potential clients by

encouraging them to opt in to receiving e-mails, including e-newsletters and information regarding promotions. If Congress or the FTC were ever to mandate a do-not-e-mail registry or similar policy, it's likely that many people would sign up. But if a business has obtained prior affirmative consent from recipients of its e-mails, then their decision to be part of any future do-not-e-mail list may not render them off-limits. Many industry and consumer groups also consider opt-in a "best practice."

The opt-out requirement may be problematic for companies that include advertisements in e-mail sent from other vendors, such as online promotional agencies, from co-promotional partners, or via viral e-mail programs. According to the law, both the sender of the e-mail and the advertiser must honor a request to unsubscribe. This means that opt-out lists should be kept by all entities involved in an e-mailing and some mechanism for ensuring uniformity should be in place.

Labeling requirements. All commercial e-mail must also include a valid physical postal address of the sender and conspicuous notice that the message is an advertisement if the recipient has not given prior affirmative consent. This summer, the FTC will

Businesses using e-mail for commercial purposes cannot afford to ignore CAN-SPAM.

decide if it will require commercial e-mails to be designated as advertisement in the subject line.

Sexually oriented material. E-mails with sexually oriented material are defined as "any material that depicts sexually explicit conduct ... unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters." These e-mails must exclude sexually oriented materials from the subject heading and include the phrase, "sexually explicit," in the heading if the recipient has not given prior affirmative consent to receipt of the message. The FTC may modify the required notification.

The e-mail body must include only the phrase, "sexually explicit," certain notices required by the CAN-SPAM Act, instructions or a mechanism for accessing the sexually oriented material, and a statement that to avoid viewing the sexually oriented material, the e-mail should be deleted and the instructions disregarded. So far, it's unclear if a simple link to the sexually explicit material will be

acceptable or if the FTC will mandate a more arduous method for access.

Mobile Messages. The Federal Communications Commission (FCC), rather than the FTC, regulates wireless spamming. Commercial e-mails sent to an Internet domain name associated with wireless subscriber messaging services are generally prohibited unless expressly authorized. All commercial mobile radio service providers are now required to submit domain names to the FCC for inclusion in a public list.

The FCC rules create potential liability for sending commercial messages to domain names that have been on the FCC list for 30 days or more, so senders of commercial e-mails should regularly check their recipient lists against the FCC list. Senders of commercial e-mail also need to ensure that they do not offer recipients payment, consideration, or other inducement to forward messages to wireless subscribers on the FCC list. To be safe, promoters offering inducements for others to forward their messages should include language expressly prohibiting others from forwarding such messages to wireless subscribers.

In the case of commercial messages to wireless subscribers that are not prohibited, the initiator of the message must still follow the protocol of the CAN-SPAM Act labeling and opt-out requirements, identify itself to allow subscribers to reasonably determine that it's the authorized entity, and ensure that a recipient who grants electronic authorization to receive commercial e-mail has the option, with clear and conspicuous instructions, to reject further messages by the same electronic means used to obtain authorization. Furthermore, the sender must ensure that at least one opt-out method, either the electronic means for rejecting further messages or a reply to the opt-out address, will not result in additional charges to a subscriber.

Prohibition of deceptive e-mails. The CAN-SPAM Act makes it illegal to misappropriate another e-mail server to traffic in commercial e-mails; falsify or disguise e-mail addresses or headers to obscure identity or avoid filters; use subject headings that are deceptive or misleading; or register for or misappropriate multiple e-mail addresses using false identities to engage in commercial e-mailing.

Most of the activities listed here have already been prohibited by other legislation and/or FTC regulations and enforcement actions, so this section of the new CAN-SPAM Act should come as no surprise.

Address harvesting. In an effort to control boiler room spam operations, CAN-SPAM prohibits sending e-mails using a system that generates e-mail addresses by automatically combining names, letters, or num-

bers or searching or registering for e-mail accounts using such an automated system. CAN-SPAM also makes it illegal to use automated means to search a Web site or proprietary online service for e-mail addresses if the Web site or service includes a notice that the operator will not sell or transfer addresses to any other party for commercial purposes. It's recommended that all Web site terms of use specifically prohibit use of bots, spiders, and scrapers to collect e-mail addresses and other content from the site.

E-mail harvesting has long been the domain of professional spammers. However, businesses that do not spam but do send messages based on electronically generated addresses (e.g., offers to other Web entities for reciprocal linking partnerships) may violate the law if any of the Web sites they scan contain language prohibiting the capturing of addresses or content. Furthermore, businesses can be held liable under CAN-SPAM if they knowingly use lists from other parties that were generated illegally.

Even using e-mail addresses of unknown origin may be held to violate the CAN-SPAM Act. CDs filled with e-mail addresses and lists of e-mail addresses accessed at below-market rates or from unknown third parties could be viewed by the FTC as providing constructive notice that they were illegally harvested.

Affiliate liability. CAN-SPAM creates affiliate liability in an attempt to target entities that benefit from violations by partners, vendors, and others that send e-mails on their behalf. It's illegal for a person to promote or allow the promotion of that person's business by e-mails that violate other provisions in the CAN-SPAM Act if that person (1) knew or should have known that the business was being promoted by means of such a message; or (2) received or expected to receive economic benefit from the promotion, and took no reasonable action to prevent or detect and report the transmission.

The act does place some limitations on affiliate liability for companies that merely provide goods or services to another party that violates CAN-SPAM. Generally, a third party that provides property, goods, or services to an entity that violates the act will not be held liable for that entity's violation unless the third party owns more than a 50% interest in the trade or business of the entity that violates the act or the third party has actual knowledge that property, goods, or services are promoted in a commercial e-mail message that violates the act and receives or expects to receive economic benefit from the promotion. This exception, in most cases, does

not help advertising and promotional agencies or their clients.

For many legitimate businesses, this may be the most troubling part of the CAN-SPAM Act. They may not engage in illicit activity, but they may have willingly allowed "affiliates" to promote their product or service via e-mail or viral e-mail campaigns. It's best to set out clear, protective provisions in any vendor agreement with entities that will advertise over the Internet, particularly via viral e-mail and e-mail blasts, or engage others to do so. A provision for termination in the event of unauthorized e-mailing is advisable. Vendors should be required to defend, indemnify, and hold harmless. Special concern should be given to use of viral e-mail promotions, so seek legal advice when planning such a promotion, in order to design a program that does not create affiliate liability.

Penalties

The punishments for violation of the CAN-SPAM Act can be stiff, including "per violation" fines up to \$6 million and prison terms up to five years. In the initial months following promulgation of the CAN-SPAM Act, compliance actions were low, although enforcement is now picking up steam. The FTC, however, simply lacks the capacity to respond to the more than 300,000 spam-related complaints it receives daily, and service providers likely will primarily target the most egregious offenders when bringing private actions. Businesses not in compliance that are not purposeful or egregious violators likely have the opportunity to clean up their act if they act quickly. It's highly advisable that they do. Anti-spam regulation and technologies will probably evolve quickly, with many observers, including Microsoft's Bill Gates, predicting major breakthroughs in the next two years. Businesses that take action now will be poised to succeed in this new environment and avoid costly legal problems in the future. ■

Author's note: Research assistance was provided by Steven Wright, Kaye Scholer Associate. This article does not constitute legal advice.

About the Author

Alan L. Friel is counsel in the Los Angeles office of international law firm Kaye Scholer LLP, where he practices in the areas of advertising, entertainment, and technology law. He may be reached at AFriel@KayeScholer.com.