

THE NEW FEDERAL SPAM LAW: YOU'RE LIKELY NOT IN COMPLIANCE

By Jacob C. Reinbolt
Procopio, Cory, Hargreaves & Savitch LLP

Effective January 1, 2004, the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (the "CAN-SPAM Act") will attempt to deal with "spam" email. Paradoxically, however, the new law does not prohibit unsolicited commercial email, which is what most people consider "spam."

The new law will attempt to control unsolicited commercial email by, among other things, requiring that such email: (i) clearly identify itself as an advertisement; (ii) include opt-out instructions; and (iii) contain the sender's physical address.

State laws that require labels on unsolicited commercial email, or that prohibit such email entirely, are preempted, although, importantly, state law provisions dealing with falsity, deception, and fraudulent activities remain effective.

While the new law contains a number of ambiguities and uncertainties, certain steps can be taken by legitimate commercial business to try to comply with the law. Those steps are highlighted below as "*Compliance Points*."

I. **Types of Email Regulated.**

The CAN-SPAM Act allows companies to send unsolicited email ads so long as certain requirements are met.

A. **"Commercial Electronic Mail Messages."**

The new law's main emphasis is on the term "commercial electronic mail message," which is defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service . . ."

Unfortunately, the terms "primary purpose," "advertisement," and "promotion," are not currently defined. The FTC is required to issue regulations by December 2004 "defining the relevant criteria to facilitate the determination of the primary purpose" of an email.

Compliance Point: Until the term "primary purpose" is clarified, businesses will need to err on the side of compliance even if a particular email may be exempted because its "primary purpose" is not to "advertise or promote" a "product or service."

B. **"Transactional or Relationship Messages."**

The new law provides an exemption in certain instances for "transactional or relationship messages." "Transactional or relationship messages" include e-mails the primary purpose of which is:

- i. to facilitate a commercial transaction that the recipient has previously agreed to enter into with the sender;

- ii. to provide warranty information, product recall information, or safety information with respect to a commercial product or service used or purchased by the recipient;
- iii. to provide: (a) notification concerning a change in the terms or features of; or (b) at regular periodic intervals, account information with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;
- iv. to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

This defined term is important because certain prohibitions apply only to "commercial electronic mail messages."

II. Requirements for Regulated Emails.

A. False or Misleading Transmission Information.

Neither "commercial electronic email messages" nor "transactional and relationship messages" may be sent if the message "contains, or is accompanied by, header information that is materially false or misleading." "Materially false or materially misleading" is defined as: (i) header information that is technically accurate but includes an originating email address or domain name that was obtained by means of false or fraudulent pretenses; and (ii) header information that fails to identify a computer used to initiate the message because the initiator used another computer to relay the message for purposes of disguising its origin.

B. Deceptive Subject Headings.

It is unlawful to initiate the transmission of a "commercial electronic mail message" (but, oddly, not a "transaction or relationship message") if the sender has knowledge that a subject heading of the message would be likely to mislead a recipient about the contents or subject matter of the message.

Compliance Point: Companies must ensure that the subject headings they use are not inadvertently deceptive. The use of "creative" subject headings to encourage recipients to open emails they would otherwise delete may result in liability.

C. Opt-Out Requirements.

Recipients of commercial electronic mail messages must be provided a means to "request not to receive" future emails from the senders of those emails. Such "opt-out" mechanism must be a return electronic mail address or other Internet-based mechanism that is clearly and conspicuously displayed that allows the recipient to indicate it does not want to receive future emails from that sender at the electronic mail address where the message was received.

Compliance Point: The opt-out requirement applies to even single email transmissions, in addition to "mass" emailings. Consequently, companies need to ensure that their employees understand what a "commercial electronic mail message" is so that the requirements applicable to such emails are complied with in all instances.

The opt-out opportunity must permit recipients to refuse future emails from the sender - i.e., the entity whose product or service is advertised - rather than from a "non-sender" initiator, if one was used.

The Act allows more detailed opt-out options. For example, recipients can be provided with a list or menu to choose the types of emails they do or do not want to receive from the sender, if this menu also includes an option to opt-out from receiving all emails from the sender.

Opt-out requests must be complied with within 10 business days after they are received.

Compliance Point: While an unsolicited commercial email can be sent to anyone, this will potentially be a one-time opportunity. All "commercial electronic mail messages" companies send must contain the required, functioning, opt-out mechanism that is clearly and conspicuously displayed. Opt-out requests must be complied with within 10 business days after receipt by the sender. Companies will need to put procedures in place to meet the 10 day opt-out deadline.

D. **Advertisement Identifier, Opt-Out Notice, and Address Requirements.**

The new law requires senders to provide in each "commercial electronic mail message" email: (i) "clear and conspicuous identification that the message is an advertisement or solicitation;" (ii) "clear and conspicuous notice of the opportunity" to opt-out from receiving further emails from the sender; and (iii) "a valid physical postal address of the sender."

If the recipient has given "prior affirmative consent to receipt of the message" then the message need not contain the "clear and conspicuous identification that the message is an advertisement or solicitation," but must still include notice of the opt-out opportunity and a valid postal address of the sender.

Compliance Point: If the emails a company sends fall within the definition of a "commercial electronic mail message" then it will need to be sure to include the necessary identification, notice, and address information. Since "clear and conspicuous" is not defined, companies will need to exercise some judgment on this point.

III. **State Anti-Spam Laws Generally Are Preempted.**

The CAN-SPAM Act "supersedes any statute, regulation, or rule of a state or political subdivision of a state that expressly regulates the use of the electronic mail to send commercial messages, **except to the extent that** any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." This provision is intended to protect legitimate businesses against more restrictive state legislation.

Compliance Point: The misimpression that many people harbor that state anti-spam laws are completely preempted is inaccurate. State law fraud, deception, and unfair competition causes of action, among others, remain viable.

IV. **Aggravated Violations.**

The Act defines certain actions as aggravated violations for which penalties may be increased. Aggravated violations include:

1. Initiating the transmission of an email, or assisting in the "origination" of the email, if the recipient's email address was obtained using an automated means that generates possible email addresses;
2. Using automated means to register for multiple email accounts or online user accounts from which to transmit an unlawful email; and
3. Relaying of an unlawful email from a computer or computer network that was accessed without authorization.

Compliance Point: Because this aggravated liability applies to those who "assist in the origination of the email message" if they had actual knowledge, or "knowledge fairly implied on the basis of objective circumstances" of the violation, companies that hire third parties to send emails on their behalf will need to assess how the email addresses were obtained.

V. **Enforcement.**

The new law will be enforced by the FTC, state attorney general actions, criminal prosecutions, and private suits brought by Internet service providers. The FTC has the authority to impose monetary penalties and refer violations to the Department of Justice for criminal prosecution.

Providers of Internet access service may also bring a private action if they have been adversely affected by certain violations of the law.

VI. **Continuing FTC Rule-Making.**

In addition to the FTC's obligation to define the "primary purpose" of an email, the FTC has other rule-making and clarification obligations.

. **Reward System.**

By September 2004, the FTC is required to prepare a report that sets forth a system for rewarding those who supply information about violations of the new law, including procedures for the FTC to grant a reward of at least 20% of the total civil penalty collected for a violation of the law to the first person who reports the violation.

Compliance Point: Once these reward provisions are in place, "whistleblowing" will likely increase. Thus, companies will at that time need to be even more vigilant in attempting to comply with the law.

A. **Establishment of Identification for Commercial Email.**

Within 18 months of enactment, the FTC is required to create a plan for requiring commercial electronic mail messages to be identifiable from their subject line, such as by use of identifiers like "ADV."

In addition to these required actions (and those described previously), the new law gives the FTC the discretion to modify or expand the Act's requirements by issuing regulations on certain issues.

Compliance Point: Because of the FTC's responsibilities and discretion, regular monitoring of the FTC's actions will be required to ensure continuing compliance with the law's evolving standards.