The CAN-SPAM Act: Requirements for Commercial Emailers

The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them.

The law, which became effective January 1, 2004, covers email whose primary purpose is advertising or promoting a commercial product or service, including content on a Web site. A "transactional or relationship message" – email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship – may not contain false or misleading routing information, but otherwise is exempt from most provisions of the CAN-SPAM Act.

The Federal Trade Commission (FTC), the nation's consumer protection agency, is authorized to enforce the CAN-SPAM Act. CAN-SPAM also gives the Department of Justice (DOJ) the authority to enforce its criminal sanctions. Other federal and state agencies can enforce the law against organizations under their jurisdiction, and companies that provide Internet access may sue violators, as well.

What the Law Requires

Here's a rundown of the law's main provisions:

It bans false or misleading header information. Your email's "From," "To," and routing information – including the originating domain name and email address – must be accurate and identify the person who initiated the email.

It prohibits deceptive subject lines. The subject line cannot mislead the recipient about the contents or subject matter of the message.

It requires that your email give recipients an opt-out method. You must provide a return email address or another Internet-based response mechanism that allows a recipient to ask you not to send future email messages to that email address, and you must honor the requests. You may create a "menu" of choices to allow a recipient to opt out of certain types of messages, but you must include the option to end any commercial messages from the sender.

Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your commercial email. When you receive an opt-out request, the law gives you 10 business days to stop sending email to the requestor's email address. You cannot help another entity send email to that address, or have another entity send email on your behalf to that address. Finally, it's illegal for you to sell or transfer the email addresses of people who choose not to receive your email, even in the form of a mailing list, unless you transfer the addresses so another entity can comply with the law.

It requires that commercial email be identified as an advertisement and include the sender's valid physical postal address. Your message must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial email from you. It also must include your valid physical postal address.

Penalties

Each violation of the above provisions is subject to fines of up to $11,000. Deceptive commercial email also is subject to laws banning false or misleading advertising.

Additional fines are provided for commercial emailers who not only violate the rules described above, but also:

- "harvest" email addresses from Web sites or Web services that have published a notice prohibiting the transfer of email addresses for the purpose of sending email
- Generate email addresses using a "dictionary attack" – combining names, letters, or numbers into multiple permutations
- Use scripts or other automated ways to register for multiple email or user accounts to send commercial email
- Relay emails through a computer or network without permission – for example, by taking advantage of open relays or open proxies without authorization.

The law allows the DOJ to seek criminal penalties, including imprisonment, for commercial emailers who do – or conspire to:

- Use another computer without authorization and send commercial email from or through it
- Use a computer to relay or retransmit multiple commercial email messages to deceive or mislead recipients or an Internet access service about the origin of the message
- Falsify header information in multiple email messages and initiate the transmission of such messages
- Register for multiple email accounts or domain names using information that falsifies the identity of the actual registrant
- Falsely represent themselves as owners of multiple Internet Protocol addresses that are used to send commercial email messages.

Additional Rules

The FTC will issue additional rules under the CAN-SPAM Act involving the required labeling of sexually explicit commercial email and the criteria for determining "the primary purpose" of a commercial email. Look for the rule covering the labeling of sexually explicit material in April 2004; "the primary purpose" rulemaking will be complete by the end of 2004. The Act also instructs the FTC to report to Congress in summer 2004 on a National Do Not E-Mail Registry, and issue reports in the next two years on the labeling of all commercial email, the creation of a "bounty system" to promote enforcement of the law, and the effectiveness and enforcement of the CAN-SPAM Act.

See the FTC Web site at www.ftc.gov/spam for updates on implementation of the CAN-SPAM Act.

The FTC maintains a consumer complaint database of violations of the laws that the FTC enforces. Consumers can submit complaints online at www.ftc.gov and forward unwanted commercial email to the FTC at spam@uce.gov.