

## The CAN-SPAM Act: How it Affects You

The widely publicized “CAN-SPAM Act of 2003”<sup>1</sup> became effective on January 1, 2004, just weeks after it was signed by President George W. Bush. The CAN-SPAM Act is intended to create one national standard of spam regulation and applies not only to the person or entity sending the commercial e-mail message but also to the person or entity advertising in such message. The CAN-SPAM Act preempts state laws that expressly regulate the use of e-mail to send commercial messages, except to the extent that such laws prohibit the sending of false or deceptive e-mail messages. To help you prepare to comply with this new law, this alert summarizes the main parts of the CAN-SPAM Act.

While it remains lawful to use e-mail, even unsolicited e-mail, to advertise a commercial product or service, the CAN-SPAM Act prohibits certain deceptive or misleading practices used by some e-mail marketers and sets forth certain affirmative steps e-mail marketers must take to lawfully send commercial e-mail messages. The Act provides for criminal penalties for more nefarious spamming activities (i.e., the criminal offenses described below), as well as civil penalties for a broader range of spam-related activities (i.e., the civil violations described below).

### E-Mails Subject to the Act

The provisions of the CAN-SPAM Act generally apply only to “commercial electronic mail messages” sent by a person or entity engaging in interstate or foreign commerce.

A commercial electronic mail message (“commercial e-mail message”) is defined as “any e-mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.”<sup>2</sup>

“Transactional or relationship messages” are excluded from this broad definition of commercial e-mail messages. Except for the first violation described under the heading “Civil Violations” below, the Act does not apply to transactional or relationship messages.<sup>3</sup> A “transactional or relationship message”<sup>4</sup> is an e-mail message the primary purpose of which is:

- ▶ To facilitate, complete, or confirm a previously agreed upon commercial transaction;
- ▶ To provide warranty, product recall, or product safety or security information with respect to a commercial product or service used or purchased by the recipient;
- ▶ To provide notification concerning a change in terms or features, notification of a change in recipient’s standing or status, account balance information, or any type of account statement with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship;
- ▶ To provide information directly related to an employment relationship or employee benefit plan in which the recipient is participating; or
- ▶ To deliver goods or services (including upgrades) that the recipient is entitled to receive under the terms of a prior transaction.

### Criminal Offenses

Section 4 of the CAN-SPAM Act prohibits the following activities (as criminal offenses) in connection with sending commercial e-mail messages:

- ▶ Accessing a “protected computer”<sup>5</sup> without authorization and intentionally initiating the transmission of multiple commercial e-mails from that computer;
- ▶ Using a protected computer to relay or retransmit multiple commercial e-mails, with the intent to deceive or mislead recipients or any Internet access service, as to the origin of the messages;
- ▶ Materially falsifying header information in multiple commercial e-mail messages with the intent to deceive or mislead recipients or any Internet access service as to the origin of those messages;
- ▶ Registering domain names or creating e-mail accounts that materially falsify the

### Key Attorney Contacts

|                |                                     |
|----------------|-------------------------------------|
| Steve Dupont   | 720/566-4017<br>dupontsn@cooley.com |
| Gary Moore     | 650/843-5438<br>gmoore@cooley.com   |
| Randy Sabett   | 703/456-8137<br>rsabett@cooley.com  |
| Charles Schwab | 650/843-5347<br>schwabca@cooley.com |

This information is a general description of the law and is not intended to provide specific legal advice.

Copyright © 2004 Cooley Godward LLP, 3000 El Camino Real, Palo Alto, CA 94306. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley Godward LLP as the author. All other rights reserved.

identity of the registrant and then sending e-mails from those accounts or domain names; or

- ▶ Falsely representing oneself to be the registrant of five or more Internet Protocol addresses, and using those addresses to initiate the transmission of multiple commercial electronic mail messages.

Penalties for criminal offenses under Section 4 of the Act include fines, imprisonment, and forfeiture of any property traceable to gross proceeds obtained from the offense.<sup>6</sup>

### Civil Violations

In addition to the criminal offenses described above, the Act also establishes civil violations with respect to sending e-mail messages. Specifically, Section 5(a) of the CAN-SPAM Act includes the following prohibitions and affirmative requirements.

#### False and Misleading Header Information

The Act prohibits materially false or misleading header information in a commercial e-mail message or a *transactional or relationship message*. Header information is considered materially false or misleading if (a) it includes an originating e-mail address, domain name, or IP address that was fraudulently acquired, (b) it disguises the identity of the computer from which it originated, or (c) the “from” line does not accurately identify the initiator (i.e., the person who transmits the message or the person on whose behalf the message is sent) of the message.

#### Deceptive Subject Headings

The Act prohibits a person from initiating the transmission of a commercial e-mail message if that person has or should have actual knowledge that the subject heading of the message would be likely to mislead the recipient about a material fact regarding the contents or subject of the message.

#### Opt-Out Opportunity

The Act requires that commercial e-mail messages include a clear and conspicuous<sup>7</sup> opportunity for recipients to opt out of

receiving future commercial e-mail messages from the sender. The opt-out mechanism may be (1) a functioning e-mail address to which the recipient may send an opt-out reply, or (2) a hyperlink to a menu listing types of commercial e-mail messages sent by the sender, with an opportunity for the recipient to affirmatively indicate on such menu the types of messages he or she does or does not want to receive.

#### No Additional Messages After Opt-Out

The sender is prohibited from sending another commercial e-mail message to a recipient who has opted out more than 10 business days after receipt of the opt-out request. Should a recipient opt out of receiving some or any future commercial e-mail messages from the sender, the sender is prohibited from disclosing the recipient’s e-mail address to any other party for any purpose other than complying with the Act or other provision of law.

#### Other Required Content

The Act also requires commercial e-mail messages to contain (1) a clear and conspicuous identification that the message is an advertisement or solicitation (unless the recipient has given prior affirmative consent to receive such messages); and (2) the sender’s valid physical postal address.

#### Aggravating Activities

The CAN-SPAM Act also prohibits certain activities that aggravate the violations described above, including engaging in any of the following activities in connection with the violations above: address harvesting, dictionary attacks, automated e-mail account creation, and relay or retransmission of e-mails through unauthorized access. Specifically, it is unlawful to send a commercial e-mail message to an e-mail address that the e-mail initiator knows, or should have known, (1) was harvested from a third party’s website or online service without authorization, or (2) was generated through an automated process of combining words, letters, or numbers into numerous permutations.

### Sexually Oriented Material

Senders of commercial e-mail messages containing sexually oriented material have a separate set of content requirements with which they must comply.

#### Benefits From False or Misleading Header Information

Section 6 of the Act prohibits a person or entity from promoting, or allowing the promotion of, that person’s or entity’s goods or services through the use of commercial e-mail messages that include false or misleading header information (as described above), if the person or entity (1) knows or should have known that its goods or services are being promoted in such an e-mail, (2) received or expected to receive an economic benefit from the promotion, and (3) took no reasonable action to prevent such e-mails or detect such emails and report them to the FTC. Enforcement of this section of the Act is limited to the FTC (and other federal agencies).

### Suits Under The Can-Spam Act

#### Who Can Sue

The Act empowers a number of federal agencies, including the Federal Trade Commission (FTC), to bring enforcement actions under the Act. In addition, states and Internet access service<sup>8</sup> providers may, with certain exceptions, sue violators of the CAN-SPAM Act. The Act does not provide for a general private cause of action for persons that receive commercial e-mail messages. However, since the Act does not fully pre-empt state law, state-law-based ‘spam’ suits may persist.

#### Potential Damages

As an example of potential federal agency remedies, the FTC may seek injunctive relief and/or penalties for a violation of the Act, just as if such violation were an unfair or deceptive act or practice under the FTC Act. States and Internet access service providers may seek injunctions and may recover from violators of the CAN-SPAM Act either (a) the actual monetary loss suffered by

residents of the state or users of the Internet access service; or (b) statutory damages.

Statutory damages are calculated by multiplying the number of violations by up to \$250 (or, in the case of Internet access service providers, by up to \$100). Each separately addressed unlawful e-mail message received by residents (or, in the case of Internet access service providers, each message transferred or attempted to be transferred over the facilities of the provider) is considered a separate violation, so statutory damages can mount rapidly.

Statutory damages are generally capped at \$2,000,000 for actions brought by states and \$1,000,000 for actions brought by Internet access service providers.<sup>9</sup> However, a court may increase a damage award to three times those caps if the court determines that (1) the defendant violated the Act willfully and knowingly or (2) the unlawful activity included one or more of the activities described above in the section titled "Aggravating Activities."

### Who Can Be Sued

The CAN-SPAM Act applies not only to the person or entity sending the commercial e-mail message (i.e., the initiator), but also to the person or entity advertising in the message (i.e., the business on whose behalf the initiator is sending the e-mail). Each of the parties may be considered to be an "initiator" of a commercial e-mail message, and thus both parties should be concerned about compliance with all aspects of the CAN-SPAM Act.

## Forthcoming Regulations and Reporting Obligations

### Federal Trade Commission

The CAN-SPAM Act tasks the Federal Trade Commission ("FTC") with submitting several reports to Congress, including:

- ▶ By mid-June 2004, a report to Congress that sets forth a timetable for establishing a nationwide "Do-Not-E-mail" registry similar in function to the "Do-Not-Call" registry used to regulate the telemarketing industry. The report will also

include any practical or technical concerns the FTC has with implementing the registry. The FTC may implement the registry no earlier than mid-September 2004.

- ▶ By mid-September 2004, a report to Congress that sets forth a reward system for individuals who supply information about violations of the CAN-SPAM Act and such system must include a procedure for awarding not less than 20% of the total civil penalty collected for violations.
- ▶ By June 2005, a report to Congress that sets forth a plan to require commercial e-mail messages to be identifiable from its subject line (i.e., the use of "ADV" or a comparable identifier).

### Federal Communications Commission

The CAN-SPAM Act requires the Federal Communications Commission ("FCC"), to promulgate rules governing the use of wireless e-mail devices and "mobile service commercial e-mail." The rules are expected to allow subscribers to avoid receiving mobile service commercial e-mail, through either an opt-out regime or an opt-in regime. While the Act instructs the FCC to provide subscribers with an opt-in regime, the FCC is to take into consideration the relationship between service providers and subscribers. This means that in some cases an opt-out regime may suffice.

### Conclusion

The CAN-SPAM Act establishes the scope of liability for advertising via commercial e-mail messages, and imposes additional requirements for sending such messages. Violators risk enforcement actions brought by federal agencies (including possible criminal penalties) as well as civil suits brought by states or Internet access service providers.

Cooley Godward LLP advises clients to review their current privacy policies and e-mail advertising practices to comply with the CAN-SPAM Act. Please contact an attorney in Cooley's Technology Transactions Group for updated information and further counsel on this matter. ■

## Notes

<sup>1</sup> The "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" was signed on December 16, 2003, by President George W. Bush. The Act will be codified at 18 U.S.C. 1037.

<sup>2</sup> Unlike most state laws, the operative portion of the CAN-SPAM Act does not specifically refer to "unsolicited" e-mail messages. Rather, it describes criminal offenses and civil violations with respect to "commercial electronic mail messages."

<sup>3</sup> Only Section 5(a)(1) of the Act applies to "transactional or relationship messages" as well as to "commercial e-mail messages."

<sup>4</sup> The Act allows the Federal Trade Commission to expand or contract the types of e-mail messages that fall under the definition of "transactional or relationship message."

<sup>5</sup> Protected computer means either a computer used by the U.S. Government or a computer connected to the Internet - virtually any computer. This definition includes computers located outside the United States as long as the computer is used in a manner that affects interstate or foreign commerce.

<sup>6</sup> The Act also provides for the U.S. Sentencing Commission to consider enhanced sentences for the following actions: harvesting e-mail addresses without authorization, randomly generating e-mail by computer, and providing false registrant information to an Internet domain registrar. Finally, sentences can be increased if a violator has previously been convicted for such offenses as fraud, identity theft, obscenity, and child pornography.

<sup>7</sup> Unfortunately, the Act does not make clear what constitutes "clear and conspicuous."

<sup>8</sup> "Internet access service" means a service that enables users to access content, information, electronic mail, or other services offered over the Internet.

<sup>9</sup> The damage caps do not apply to materially false or materially misleading header information violations.