

BOSTON
WASHINGTON
NEW YORK
RESTON
NEW HAVEN
LOS ANGELES
LONDON

www.mintz.com

*One Financial Center
Boston, Massachusetts 02111 USA
617 542 6000
617 542 2241 fax*

*701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004 USA
202 434 7300
202 434 7400 fax*

*666 Third Avenue
New York, New York 10017 USA
212 935 3000
212 983 3115 fax*

*12010 Sunset Hills Road
Reston, Virginia 20190 USA
703 464 4800
703 464 4895 fax*

*157 Church Street
New Haven, Connecticut 06510 USA
203 777 8200
203 777 7111 fax*

*Water Garden
1620 26th Street
Santa Monica, California 90404 USA
310 586 3200
310 586 3202 fax*

*The Rectory
9 Ironmonger Lane
London EC2V 8EY ENGLAND
+44 (0)207 726 4000
+44 (0)207 726 0055 fax*

Client Alert

December 22, 2003

BUSINESS AND FINANCE

CAN-SPAM Act of 2003 Signed into Law by President Bush: Sets First "National Standards" for Commercial E-Mail

If your business sends any "commercial electronic mail messages" at all, the new CAN-SPAM Act of 2003, signed into law by President Bush on December 16, 2003, is likely to affect the way you send that mail.

The new law becomes effective on January 1, 2004, and will regulate any e-mail whose primary purpose is to commercially advertise or promote a commercial product or service (including content on a web site operated for commercial purposes). Certain types of e-mail which follow a transaction or relationship with the recipient are protected from penalties. Unlike the "opt-in" consent provisions of the controversial California state law which had been slated to go into effect on January 1, the new federal legislation adopts the less stringent "opt-out" approach — commercial e-mail is permitted unless and until a recipient takes affirmative action to stop it.

Companies or individuals who violate the new statute could face fines, imprisonment, disgorgement of proceeds obtained from the offense, and forfeiture of the equipment and technology used to commit the offense.

The new law preempts various state anti-spam laws, including more stringent regulations in California and Delaware. No comprehensive federal commercial e-mail law previously existed.

Protections for Users of Commercial E-Mail

The legislation provides the following:

- **False or misleading transmission information is prohibited.** It is unlawful to send false or misleading source, destination and routing information. Header information could be technically accurate but materially misleading.
- **Deceptive subject headings are prohibited.** It is unlawful to send a commercial e-mail containing a misleading subject line if the sender knew or should have known the subject was likely to mislead a recipient.
- **Message must contain a return address.** It is unlawful to send a commercial e-mail without a return address that remains functional

for 30 days after the transmission. The return address must enable the recipient to request not to receive future commercial e-mails. Certain lists or menus allowing the recipient to choose which, if any, e-mails to receive are allowed.

- ***Transmitting commercial e-mail after recipient's objection is prohibited.*** Beyond ten business days after a recipient has requested not to receive commercial e-mail from a sender, it is unlawful for either the sender or anyone acting on behalf of the sender to transmit commercial e-mail to the recipient. Once the recipient makes a request not to receive commercial e-mails from the sender, it becomes unlawful for the sender to sell, lease, or otherwise transfer the recipient's e-mail address.
- ***E-mail must contain identifier, opt-out and sender's physical address.*** A commercial e-mail is unlawful if it does not contain a clear identification that it is an advertisement or solicitation, clear and conspicuous notice that the recipient may decline to receive future commercial e-mails from the sender, and a valid physical postal address for the sender. If the recipient has given "prior affirmative consent" to the receipt of a message, then the message need not bear the "clear and conspicuous identification that the message is an advertisement or solicitation." Even where affirmative consent was given, however, the message still must include

notice of the opt out opportunity and a valid postal address of the sender.

Senders of commercial messages will not be able to avoid the requirements of the Act by using third party mailers to send unsolicited commercial e-mail on their behalf. The law prohibits a person from allowing a third party to use any of the prohibited spamming techniques to promote the advertiser's business.

Certain violations of the CAN-SPAM Act may be treated by a court as "aggravated violations," subject to up to three times the allowable damages (from a maximum of \$2,000,000 to a maximum of \$6,000,000). The following can render an offense an aggravated violation:

- ***Address Harvesting.*** Using an automated means to obtain e-mail addresses from an Internet web site or online service operated by another person which assures users that their addresses will not be sold or transferred to another party.
- ***Dictionary Attacks.*** Obtaining the recipient's e-mail address by using automated means to combine names, letter and numbers into numerous permutations.
- ***Automated Creation of Multiple E-Mail Accounts.*** Using scripts or other automated means to create multiple e-mail accounts from which to send unlawful commercial e-mails.
- ***Relay or Retransmission through Unauthorized Access.*** Knowingly

retransmitting or relaying unlawful commercial e-mails through a computer or computer network without authorization.

E-mail containing sexually oriented material must contain a mark or notice, which the Federal Trade Commission (FTC) will prescribe in the near future, in order to inform the recipient of the sexual nature of the e-mail. The immediately viewable matter in the e-mail may only contain the mark or notice, instructions on how to access the sexually oriented material, and the sender's identifier, opt-out choices and physical address. The penalty for violation is a fine or up to five years in prison, excepting prior affirmative consent by the recipient.

Third parties who have not committed the above offenses may nevertheless violate the statute if they:

- have greater than 50 percent ownership of the entity that committed the violation; **or**
- have actual knowledge of the violation **and** received, or expect to receive, an economic benefit from the violation.

Enforcement

The CAN-SPAM Act allows enforcement by the FTC, state or federal government, Internet Service Providers (ISPs) and in certain circumstances other federal agencies. Clients should beware that the FTC will be able to obtain a cease-and-desist order or an injunction without having to show that the defendant knew of the offense.

Similarly, the states will not be required to show the defendant's knowledge in order to obtain an injunction.

States may also sue for money damages, on the order of up to \$250 for each violation. (Each separately addressed e-mail would be a violation.) The maximum award is \$2,000,000. However, the court may consider certain factors to increase or reduce damages. The court may award aggravated damages up to three times the award, up to the maximum of \$6,000,000. Conversely, there are specific practices and procedures a company can implement in order to allow the court to reduce damages. ISPs may sue for an injunction or for money damages, up to \$3,000,000.

The state anti-spam statutes will be superseded by the new law. The California statute allowed individuals to sue for violations. Individuals may

not sue under the CAN-SPAM Act. The California statute also prescribed an opt-in list, which the commercial e-mail senders would be required to consult for interested recipients. The new federal law, on the other hand, will create an opt-out list, where recipients must register their e-mail addresses to indicate they would like not to receive commercial e-mails.

Predatory and Abusive Commercial E-Mail

The CAN-SPAM Act prohibits fraudulent predatory and abusive commercial email, such as:

- Unauthorized use of a computer to transmit multiple commercial e-mails
- Use of a computer to retransmit multiple commercial e-mails in order to deceive recipients or Internet access service as to their origin

- Materially falsifying header information in multiple commercial e-mails
- Registering with false identity information for five or more e-mail accounts or two or more domain names and transmitting multiple commercial e-mails
- And more

For an offense committed in furtherance of a felony, or if the offender has previously been convicted for certain computer- or e-mail-related conduct, the defendant faces a fine and/or imprisonment up to five years. First-time offenders may face a fine and/or up to three years in prison. Courts are instructed to consider the number of e-mails sent in violation of the statute as well as the dollar value of loss to recipients or gain by the offender.