NMHC
WHITE PAPERS

December 18, 2003
NMHC 03-26

CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING (CAN SPAM) ACT

By Jay Harris

Key Contacts:

James (Jay) Harris
VP of Property Management
jharris@nmhc.org

Other NMHC Staff Contacts:

Douglas M. Bibby
President
dbibby@nmhc.org

James N. Arbury
VP of Tax
jarbury@nmhc.org

Lisa E. Blackwell
VP of State & Local Outreach
lblackwell@nmhc.org

David Cardwell
VP of Housing and Finance
dcardwell@nmhc.org

Kimberly D. Duty
VP of Communications
kduty@nmhc.org

Eileen C. Lee
VP of Environment
elee@nmhc.org

Ronald G. Nickson
VP of Building Codes
rnickson@nmhc.org

Mark Obrinsky
VP of Research and Chief Economist
mobrinsky@nmhc.org

- The CAN-SPAM Act is a new federal law prohibiting "spam" or unsolicited commercial e-mail. The measure will affect a wide range of apartment marketing activities as well as communications with residents, prospects and other consumers.
- Briefly, the Act requires certain commercial e-mail messages to include valid return addresses and physical postal addresses, an opt-out option for recipients, and clear and conspicuous notice where the message is an advertisement or solicitation.
- Best practices for complying with the Act include: (1) developing model e-mails for company staff; (2) creating new procedures to track consumers who have asked to opt out of receiving certain commercial e-mail from the company and its business partners; and (3) reviewing all resident communications to determine which ones are covered by the act in light of forthcoming FTC guidelines.
- Suggested Distribution:
  - General Counsel
  - Property Management Officer
  - Chief Marketing Officer

ABOUT NMHC/NAA

Based in Washington, DC, **NMHC** represents the interests of the nation's largest and most prominent firms in the apartment industry. NMHC members are engaged in all aspects of the developing and operating apartments, including ownership, construction, management, and financing. The Council was established in 1978 as a national association to advocate for rental housing and to provide a source of vital information for the leadership of the multifamily industry. Since then, NMHC has evolved into the industry's leading national voice. The association concentrates on public policies that are of strategic importance to participants in multifamily housing, including finance, tax, property management, environmental and building codes. NMHC benefits from a focused agenda and a membership that includes the principal officers of the most distinguished real estate organizations in the United States. For more information on joining NMHC, contact the Council at 202/974-2300 or www.nmhc.org.

NAA, based in Alexandria, VA, is a federation of 155 state and local affiliated associations representing more than 28,000 members responsible for more than 4.4 million apartment homes nationwide. It is the largest broad-based organization dedicated solely to rental housing. NAA members include apartment owners, management executives, developers, builders, investors, property managers, leasing consultants, maintenance personnel, suppliers and related business professionals throughout the United States and Canada. NAA strives to provide a wealth of information through advocacy, research, technology, education and strategic partnerships. For more information, call 703/518-6141, e-mail information@naahq.org or visit www.naahq.org.

TABLE OF CONTENTS

The information discussed in this guidance is general in nature and is not intended to be legal advice. It is intended to assist owners and managers in understanding this issue area, but it may not apply to the specific fact circumstances or business situations of all owners and managers. For specific legal advice, consult your attorney.

NMHC GUIDANCE: COMPLYING WITH FEDERAL ANTI-SPAM LEGISLATION

December 2003

OVERVIEW

After years of debate, Congress has finally passed legislation banning certain unsolicited e-mails (commonly known as spam) and creating criminal penalties for violating the law. The measure, known as the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003[1] (CAN-SPAM Act), responds to public concerns about unrestricted growth of spam as well as business concerns that a uniform federal law was needed to pre-empt the existing patchwork of state laws. President Bush signed the bill into law on December 16 (P.L. 108-187), and the law will take effect January 1, 2004.

This White Paper offers operational guidance for apartment firms detailing how the measure will affect apartment firm marketing and communications with residents, prospects and other consumers. It also discusses how the law will affect trade associations' e-mail communications with their member firms.

Briefly, the CAN-SPAM Act requires commercial e-mail: (1) to be identified as advertising; (2) to include physical and electronic addresses; and (3) to include a consumer opt-out mechanism. It also makes it illegal for online marketers to disguise their identity by using a false return address or misleading subject line and prohibits senders from harvesting e-mail addresses from web sites and from many uses of e-mail addresses of individuals that have requested to opt out of receiving company e-mails. Additionally, the measure encourages the Federal Trade Commission to create a national "Do Not Spam" registry similar to the new Do Not Call registry.

Enforcement of the law will be done by the FTC, state attorneys general and Internet service providers (ISPs). Private lawsuits are not authorized. Violators can face fines of $250 per e-mail violation, up to a maximum of $2 million, though these amounts may be trebled in the case of willful or knowing violations or specified aggravated circumstances. Violators who send "fraudulent" spam can be sentenced to up to five years in prison. Also, firms that "allow" their business to be promoted through misleading commercial e-mail can, under certain circumstances, be found liable, unless they report the transmission to the Federal Trade Commission.

Importantly, the new federal law partially overrides existing anti-spam laws in some 37 states,[2] except to the extent that the state law prohibits false or deceptive commercial e-mail communications. This includes a tougher California law set to take effect January 1, 2004 that would have required online marketers to obtain a consumer's permission before sending him or her any e-mails (as opposed to the opt-out requirement in the CAN-SPAM Act[3]).

---

[1] S. 877

[2] "House Clears a Bill for Cracking Down on Spam," Wall Street Journal, D4, Dec. 9, 2003. More details on current state anti-spam laws can be found at www.spamlaws.com/state/

[3] See Calif. Bus. and Prof. Code, Div. 7, Part 3, Chap. 1, Art. 1.8, Par. 17529, 17538.45

BEST PRACTICES

As best practices to comply with the Act, member firms may want to:

1. Develop and encourage employee use of model e-mails for all corporate communication. Such a model e-mail should include:
    - accurate identification of the sender in the "From" line and the content of the message in the "Subject" line;
    - a valid physical postal address in the body of the message;
    - a clear and conspicuous notice of the opt-out feature available to the recipient; and
    - a clear identification on any message that reasonably could be construed as an advertisement or solicitation as such.

2. Implement internal systems for tracking opt-out requests from consumers, such as a centralized database and an Internet function for consumers to indicate their opt-out preferences.

3. Adopt appropriate procedures for internal reporting of any unauthorized use of consumer e-mail addresses and of any unauthorized third-party marketing about the company in violation of the Act.

4. Review resident and consumer communications in light of upcoming FTC guidelines to determine which communications constitute commercial e-mail subject to the Act's restrictions.

5. Make employees and business partners aware of the practices that the CAN-SPAM Act makes unlawful.

6. Obtain assurances from business partners that market to consumers that appropriate steps will be taken to comply with the Act.

COVERED E-MAIL

The CAN-SPAM Act generally covers "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," but not including certain "transactional or relationship messages."[4] The FTC has until December 2004 to define what constitutes the "primary purpose" of an e-mail as well as what constitutes "transactional or relationship messages" that are not covered by this law.

Until the FTC guidelines are issued, the statute specifies the following "transactional or relationship messages":

- e-mails confirming transactions that the recipient previously agreed to with the sender;
- notification of a change in terms or features or change in recipient's status with respect to certain "ongoing commercial relationship[s] involving the ongoing purchase or use by the recipients of products or services offered by the sender;"
- employment benefit plan information; or

[4] Sec. (3)(2)(A)

- the delivery of goods or services that the recipient has previously agreed to enter into with the sender.[5]

With respect to e-mails from trade associations to their respective members, the American Society of Association Executives has indicated its "understanding that communications between tax-exempt associations and charities and their respective members and donors are not affected by the new law provided that the communication is in furtherance of the organization's exempt purpose."[6]

Operations Note

E-mail marketing materials sent to recipients who did not consent to or request such e-mails will be subject to the Act. Therefore, firms may want to review their on-line marketing practices to ensure that, where possible, they are obtaining specific consent from consumers to receive future marketing communications, preferably during the consumer's initial contact with the firm's web site or e-mail system.

All commercial e-mail sent by an apartment firm should include the appropriate sender and message identifying information, opt-out features, and certain mandatory inclusions as explained under Best Practices.

Subject to future refinement by FTC regulation, an e-mail from an apartment firm to a current resident about a change in terms or features of the resident's account may be exempt from the CAN-SPAM Act's requirements below. The degree to which electronic community newsletters, account statements, notifications of new provisions of the lease or rental agreements, and other communications are covered will be determined by the forthcoming FTC regulations. Specifically, the FTC will determine the permissible balance between account information and any incidental marketing for consumers/residents who have not given their consent to receive such material. Once the FTC regulations are issued, firms may want to review their resident communications to determine those that qualify as "transactional or relationship messages" that are exempt from the CAN-SPAM Act's liability provisions.

In practice, apartment firms may choose to adopt as a matter of corporate practice the suggested requirements for transmission of messages in Section 5 of the Act (see Operations Note) for all of their communications with residents, prospects, and other consumers – even where such messages would be transactional or relationship messages not subject to the Act. It may prove easier to adopt standard corporate communication practices rather than educate employees where the Act's requirements begin and end.

SPECIFIC E-MAIL REQUIREMENTS

Section 5 of the CAN-SPAM Act imposes numerous requirements for "commercial e-mails" covered by the law. In addition, the Act's requirements also extend to other categories of e-mails, such as the prohibition of materially false identification on transactional and relationship messages as well as commercial e-mails. The requirements affect a wide range of apartment

[5] Sec. 3(17)
[6] www.asaenet.org/publicpolicy/anti-spam/

firm communications with consumers.

- Materially False Identification. The Act prohibits sending any e-mail, whether commercial or a "transactional or relationship message" with materially false or materially misleading header information. A message that accurately identifies the sender in the "From" line shall not be materially false or materially misleading.[7]

  It is also now unlawful to send commercial e-mail with a subject heading that the sender knows would likely mislead the recipient "about a material fact regarding the contents or subject matter."[8]

- Required Elements in Commercial E-Mail. Under the CAN-SPAM Act, it is unlawful for any person to transmit any commercial e-mail (to a protected computer) unless the message provides:
  - clear and conspicuous identification that the message is an advertisement or solicitation (unless the recipient has given prior affirmative consent to receive the message);
  - clear and conspicuous notice of the opportunity to opt out of receiving further commercial e-mail from the sender; and
  - the sender's valid physical postal address.[9]

- Opt-Out Requirement. The Act requires senders to allow recipients to opt out of receiving additional commercial e-mails. Specifically, it is unlawful to send commercial e-mail that does not include a clear and conspicuous return e-mail address or "Internet-based mechanism," in effect for at least 30 days after the message is sent, that the recipient can use to opt out of receiving future e-mail.[10] A recipient may subsequently give affirmative consent to receive an otherwise unlawful e-mail after requesting to opt out. [11]

  Once a recipient has opted out of receiving future messages, certain practices by the sender and related parties become unlawful. Where a recipient has opted out:
  - It is unlawful for the original sender, or a person acting on the sender's behalf, to send e-mail within the scope of the recipient's request more than 10 days after the request.[12]
  - It is unlawful for a person acting on the sender's behalf to provide or select addresses that the person knows would assist in sending a message that is within the recipient's opt-out request.[13]
  - It is unlawful for the sender, or another person who knows the recipient has made an opt-out request, to sell, lease, exchange, or otherwise transfer or release the recipient's e-mail address "for any purpose other than compliance with this Act or other provision of law."[14]

  The Act authorizes the FTC to create a Do-Not-Spam Registry similar to the existing Do-Not-Call Registry. However, the FTC has raised questions about the effectiveness of this effort.[15]

---

[7] Sec. 5(a)(1)
[8] Sec. 5(a)(2)
[9] Sec. 5(a)(5)
[10] Sec. 5(a)(3)
[11] Sec. 5(a)(4)(B)
[12] Sec. 5(a)(4)(A)(i), (ii)
[13] Sec. 5(a)(4)(A)(iii)
[14] Sec. 5(a)(4)(A)(iv)
[15] Sec. 9

The FTC is expected to report to Congress in 2004 on the feasibility of such a Registry.

Operations Note:
Firms will need to have an effective opt-out mechanism in place to identify consumers who have asked not to receive additional material from the company. Approaches will vary, but it may prove more effective to refer consumers that want to "opt out" to a centralized Internet site or e-mail address, instead of making firm employees responsible for processing or forwarding consumer opt-out requests. Note also that the e-mail address or URL provided for consumer opt-out must remain available for at least thirty days after the message is sent.

A centralized opt-out request processing function also permits the company to provide choices for residents who want to opt out of receiving various categories of company communications – for example, all company communications, all marketing communications, or simply all communications except those that apply to the property where the consumer resides.

Firms will need to establish reasonable procedures to ensure that commercial e-mails sent to consumers are not within the scope of any opt-out request a consumer has made. These procedures should address commercial e-mails sent to consumers not only by company associates, but by ancillary service providers with consumer contact as well, such as independent marketing and listing services, utility billing firms, rental insurance providers, and the like. Future FTC guidelines will help define what procedures are appropriate, but apartment firms should begin to think through how best to centralize and update opt-out requests.

As a best practice, firms may also want to develop model e-mails for corporate communication that include the following features:

1. *Accurate identification of the sender in the "From" line (that is, not borrowing the e-mail account of another to send a consumer message);*
2. *Accurate identification of the message's content in the "Subject" line in any consumer communications;*
3. *Clear and conspicuous notice of the opt-out feature available to the consumer, such as a URL to the opt-out page of the company web site or a centralized e-mail address;*
4. *On any message that reasonably could be construed as an advertisement or solicitation, a clear identification of the message as such. The statute does not require the inclusion of "ADV:" in the header of any advertising e-mail to meet the clear identification requirement;*
5. *A valid postal physical address in the body of the message. While additional clarification is needed, this provision appears to require that an actual street address is needed to meet this requirement. A post office box address may not suffice.*

LIABILITY FOR THE COMMUNICATIONS OF OTHERS

The CAN-SPAM Act also makes it unlawful for a business (e.g., an apartment firm) to promote—or to allow the promotion of—its business in materially false or materially misleading header information in violation of 5 (a)(1), as long as the business:

- knows, or should have known, the business was being promoted this way;
- received, or expected to receive, economic benefit; and

- did not take reasonable action to prevent the transmission or deter it and report it to the FTC.[16]

Operations Note:
Firms may want to encourage employees that become aware of materially false or materially misleading third-party promotions about the firm to report such promotions to their supervisor or the firm's general counsel, to ensure that the firm takes appropriate action, if necessary.

The scope of the "economic benefit" provision remains to be determined. Conceivably it is broad enough that a firm that stands to benefit by receiving additional revenue as a result of certain illegal promotions may be subject to liability under this section, even where the beneficiary apartment firm has no relationship with the sender.

PROHIBITED PRACTICES

Certain "predatory and abusive" e-mail is prohibited by the Act. While these acts are more commonly associated with egregious marketing practices not usually found in multifamily marketing, caution is advised in light of the enhanced penalties for violations. Convicted violators of these provisions are subject to imprisonment of up to five years and forfeiture of property obtained from or used to commit the offense.[17] They include the following:

1. Sending multiple commercial e-mails with unauthorized access;
2. Relaying or retransmitting multiple commercial e-mails with the intent to deceive recipients as to the origin;
3. Sending multiple commercial e-mails with materially falsified headers;
4. Registering for five or more e-mail accounts or two or more domain names using a materially falsified identity and sending multiple commercial e-mails from those accounts;
5. Falsely representing oneself to be the registrant or successor in interest to 5 or more Internet Protocol (IP) addresses and sending multiple commercial e-mails.

In addition, commercial e-mails containing sexually oriented material must contain appropriate warning labels and access restrictions.[18]

STATE LAWS AND ENFORCEMENT

Generally, the FTC has enforcement authority over rental housing activities, though an appropriate federal regulator may have independent enforcement authority over NMHC members under other applicable law (e.g., the Securities and Exchange Commission would have enforcement authority under the 1934 Securities Act).[19]

State attorneys general and Internet service providers also have authority to seek injunctions and damages (up to $2 million for attorneys general, $1 million for ISPs) for certain violations of the header and message content identifier, opt out and physical address identifier, and sexually oriented material provisions in Section 5.

[16] Sec. 6(a)(1)
[17] Sec. 4
[18] Sec. 5(d)
[19] Sec. 7(a), (b)

Damages may be trebled for willful or knowing violations or aggravated violations. The Act identifies the following automated processes as "aggravated violations":

- address harvesting and dictionary attacks;
- automated creation of multiple e-mail accounts; and
- relay or retransmission of commercial e-mail through unauthorized access.[20]

Damages may be reduced where the defendant implemented commercially reasonable practices designed to prevent these violations.[21]

The Act supersedes state and local law that expressly regulates the use of electronic mail to send commercial messages, except to the extent that the state or local law prohibits false or deceptive commercial e-mail communications.[22] A recent California statute that requires an opt-in rule for e-mail advertising is among the key state laws pre-empted by the CAN-SPAM Act. The statute, which was scheduled to take effect January 1, 2004, would have made it illegal to send unsolicited commercial e-mail from California or to a California e-mail address. The law would have applied to senders as well as to advertisers on whose behalf messages are sent.[23]

Firms should be aware that enforcement activity under state anti-fraud laws will continue. In recent state law actions for spam violations, the enforcing parties have emphasized that a broad range of spam activities will continue to be prosecuted under state spam anti-fraud laws even after the CAN-SPAM Act. For example, after the CAN-SPAM Act passed Congress, the Virginia Attorney General brought a felony indictment against e-mail promoters that used falsified router information to promote home mortgage teaser rates.[24]

CONCLUSION

In light of the potentially stiff penalties the CAN-SPAM Act provides for, member firms should note the Act's penalty reduction incentive to adopt commercially reasonable practices to prevent violations.

[20] Sec. 5(b)
[21] Sec. 7(f), (g)
[22] Sec. 8(b)
[23] See www.spamlaws.com/state/summary.html#ca
[24] "Virginia indicts two on spam felony charges," Dec. 12, 2003, http://edition.cnn.com/2003/TECH/internet/12/12/spam.charges/