



# E-mail Marketing: CAN-SPAM Act Compliance

*David J. Ervin and Christopher M. Loeffler, Kelley Drye and Warren LLP*

This Practice Note is published by Practical Law Company on its <sup>PLC</sup>Law Department web service at <http://us.practicallaw.com/0-503-5278>.

## A Note discussing the federal CAN-SPAM Act's requirements for commercial e-mails, its enforcement and best practices for compliance.

The widespread consumer acceptance of online communication provides marketers with a number of benefits compared to traditional direct marketing campaigns, including:

- Lower costs.
- Almost instantaneous delivery.
- A more interactive experience generally allowing users to immediately click through to the marketer's website.

However, the ease and efficiency of e-mail marketing also brings drawbacks. The high volume of unsolicited commercial e-mail messages (spam) received by consumers makes it difficult for individual marketers to stand out. In addition, consumers do not want their inboxes full of spam, which, in some cases, are also fraudulent or contain offensive content.

In 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act (15 U.S.C. § 7701-13) (CAN-SPAM Act) to regulate unsolicited commercial e-mail. The CAN-SPAM Act does not flatly prohibit all unsolicited commercial e-mail. Instead, it sets out specific requirements for the content of these messages and to ensure that consumers can opt out of receiving them.

This Note discusses the federal CAN-SPAM Act, including:

- The scope of the CAN-SPAM Act.
- The CAN-SPAM Act's requirements, including certain Federal

Trade Commission (FTC) and Federal Communications Commission (FCC) implementing regulations and rules.

- Enforcement of the CAN-SPAM Act, including penalties for violations.
- Best practices for marketers' compliance with the CAN-SPAM Act.

Companies using e-mail to market and advertise their products and services also must pay careful attention to compliance with other applicable laws, including, for example, other laws addressing marketing and advertising practices (for more information, see *Practice Notes, Advertising: Overview* (<http://us.practicallaw.com/2-501-2799>), *Online Marketing and Advertising* (<http://us.practicallaw.com/4-500-4232>) and *Direct Marketing* (<http://us.practicallaw.com/5-500-4203>)) and privacy and data security laws (for more information, see *Practice Notes, US Privacy and Data Security Law: Overview* (<http://us.practicallaw.com/6-501-4555>) and *Privacy and Data Security: Breach Notification* (<http://us.practicallaw.com/3-501-1474>)).

## SCOPE OF THE CAN-SPAM ACT

The CAN-SPAM Act regulates the transmission of all commercial e-mail messages, not just unsolicited messages. A commercial e-mail message is defined as any e-mail that has a "primary purpose of . . . commercial advertisement or promotion of a commercial product or service" (15 U.S.C. § 7702(2)(A)). This includes commercial e-mails sent to business e-mail accounts, as well as those sent to individual consumers.

The CAN-SPAM Act authorizes the FTC to issue regulations implementing the CAN-SPAM Act's provisions (the CAN-SPAM Rule codified at 16 C.F.R. part 316). Similarly, the FCC has authority under the CAN-SPAM Act to issue rules addressing unsolicited commercial messages sent to consumers' wireless devices (see *E-mail Sent to a Wireless Device*).

### IS IT A COMMERCIAL MESSAGE?

A first step in evaluating whether the CAN-SPAM Act applies to an e-mail message is to determine whether the e-mail is a commercial message. Not every e-mail message from a business is deemed a commercial message under the CAN-SPAM Act. Rather, the e-mail's primary purpose must be the commercial advertisement or promotion of a product or service.

In particular, messages sent to consumers that have a primary purpose relating to a particular transaction or relationship between the sender and the consumer are expressly exempted from the CAN-SPAM Act's specific requirements for commercial messages (*15 U.S.C. § 7702(2)(B)*). To qualify as a transactional or relationship message, the e-mail's primary purpose must be to do one or more of the following:

- Facilitate, complete or confirm a commercial transaction previously agreed to by the e-mail recipient.
- Provide warranty, product recall, safety or security information for a product purchased by the e-mail recipient.
- Provide certain information permitted under the CAN-SPAM Act regarding a subscription, membership, account, loan or similar ongoing relationship concerning the e-mail recipient's ongoing purchase or use of the sender's products or services (for example, notification of a change in terms or features of a membership or subscription or periodic account information).
- Provide information regarding an employment relationship or related benefit plan in which the e-mail recipient is currently involved, participating or enrolled.
- Deliver goods or services (for example, updates or upgrades) that the e-mail recipient is entitled to receive as a result of a previously agreed upon transaction.

(*15 U.S.C. § 7702(17)(A)*.)

If the message includes content only in one or more of the above categories, it is not a commercial message under the CAN-SPAM Act. If a message contains both transactional or relationship content and commercial content, the CAN-SPAM Act's commercial e-mail requirements apply if the message's primary purpose is commercial (see *Is the Message's Primary Purpose Commercial?*).

The CAN-SPAM Act also contains compliance obligations and prohibitions for transactional or relationship messages (see *Prohibition on False or Misleading Transmission Information*), but these are less rigorous than the rest of the requirements specific to commercial messages (see generally, *Commercial Message Requirements*).

### IS THE MESSAGE'S PRIMARY PURPOSE COMMERCIAL?

Even if the e-mail does include some commercial content, the CAN-SPAM Act's commercial e-mail requirements apply only if the message's primary purpose is commercial. The FTC has clarified the analysis to determine a message's primary purpose as follows:

- **Messages Containing Only Advertising Content.** These messages have a commercial primary purpose.
- **Messages Containing Both Advertising and Transactional or Relationship Content.** These messages have a commercial primary purpose if either:
  - The recipient would interpret the subject line to mean that the message contains commercial advertising.
  - A substantial part of the transactional or relationship content does not appear at the beginning of the message.
- **Messages Containing Both Advertising Content and Other Non-transactional or Non-relationship Content.** These messages have a commercial primary purpose if either:
  - The recipient would interpret the subject line to mean that the message contains commercial advertising.
  - The recipient would determine from the body of the message that the message's primary purpose is commercial advertising.

In making this determination, factors for the recipient to consider include:

- the placement of the commercial advertising at the beginning of the message;
  - the proportion of the message dedicated to commercial advertising; and
  - how prominent the commercial advertising is (for example, highlighted through use of graphics type size and style).
- **Messages Containing only Transactional or Relationship Content.** These messages do not have a commercial primary purpose (see also *Is it a Commercial Message?*).

(*16 C.F.R. § 316.3*.)

### WHO MUST COMPLY WITH THE CAN-SPAM ACT?

#### Initiators of Commercial E-mail Messages

Any person, including business entities and nonprofit associations, that initiates commercial e-mail messages must comply with the CAN-SPAM Act requirements (see *Can-Spam Act Requirements*). As defined by the CAN-SPAM Act, a person is an "initiator" of a commercial e-mail message if it either:

- Originates or transmits the e-mail.
- Procures the transmission of the e-mail, meaning that the business either intentionally pays or provides other consideration to, or induces, another person to transmit the e-mail on its behalf.

The CAN-SPAM Act contains an exception, however, when the person initiating the commercial e-mail is involved solely in routine conveyance. This is when the person's actions only relate to the transmission, routing or storage of the message through an automatic technical process and the person is not involved in identifying or providing the recipients' addresses for the message.

## Senders of Commercial E-mail Messages

Certain other requirements apply specifically to “senders” (see *Opt-Out Requirements* and *Other Requirements*). A sender is an initiator whose own product or service, or internet website, is advertised or promoted in the commercial message. A commercial e-mail can have more than one initiator or sender. For example, where a business engages a third-party service provider to send a commercial e-mail advertising the business’s products, both parties are initiators under the CAN-SPAM Act. The business is also a sender under the CAN-SPAM Act.

For specific issues involving determining whether a person is an initiator or sender under the CAN-SPAM Act, see *Common Marketing Practices: “Forward-to-a-Friend” E-mails, Multiple Senders and Affiliate Marketing*.

## CAN-SPAM ACT REQUIREMENTS

### PROHIBITION ON FALSE OR MISLEADING TRANSMISSION INFORMATION

It is a violation of the CAN-SPAM Act to initiate the transmission of a commercial message or a transactional or relationship message that contains false or misleading transmission information, which is an e-mail’s “From,” “To,” “Reply to” and routing information (also known as the header information). Instead, this information must be correct and identify the person initiating the message (15 U.S.C. § 7704(a)(1)).

### COMMERCIAL MESSAGE REQUIREMENTS

#### Prohibition on Deceptive Subject Headings

The CAN-SPAM Act prohibits a person from initiating a commercial e-mail with a deceptive subject heading. This means that the initiator of the message cannot have actual knowledge (or knowledge fairly implied under the circumstances) that the subject heading would be likely to mislead the recipient about a material fact regarding the message’s contents or subject matter (15 U.S.C. § 7704(a)(1)).

#### Opt-out Requirements

The CAN-SPAM Act requires initiators of a commercial e-mail to include following elements in each commercial e-mail:

- Clear notice of the recipient’s right to not receive (opt out of) future messages from the sender of the e-mail.
- One of the following mechanisms for opting out:
  - a functional return e-mail address, allowing the recipient to simply “reply” to the e-mail indicating the recipient’s opt out; or
  - another internet-based opt-out mechanism (for example, a link to a separate web page containing the opt-out mechanism).

The opt-out mechanism must be functional for at least 30 days after the message is sent. If the return e-mail address or other mechanism, however, is unexpectedly and temporarily unable to receive messages or process opt-out requests resulting from a

technical problem beyond the sender’s control, it is not a violation of the CAN-SPAM Act’s opt-out requirements if the problem is corrected within a reasonable time (15 U.S.C. § 7704(a)(3)(C)).

A sender of a commercial e-mail cannot require the recipient to do any of the following to submit (or have the sender honor) an opt-out request when using any of the opt-out methods required by the CAN-SPAM Act:

- Pay a fee.
- Provide any information other than the recipient’s e-mail address and opt-out preferences.
- Take any steps other than sending a reply message or visiting a single website.

(16 C.F.R. § 316.5.)

If the message recipient submits a request to opt out of receiving future message from a sender, all of the following apply:

- The opt out must become effective within 10 business days. After this time, the sender (or anyone on its behalf) may not send further commercial e-mail messages falling within the scope of the opt-out request to that recipient, unless the recipient subsequently requests to receive (opts in) these messages.
- The opt out never expires.
- The sender (and any other person that knows the recipient has opted out of further commercial messages) cannot sell, exchange or otherwise transfer the recipient’s e-mail address except as required by law unless that recipient has explicitly opted in to permitting the sale, exchange or transfer.

(15 U.S.C. § 7704(a)(3)-(5)(A)(i)-(iv).)

#### Other Requirements

Initiators of a commercial e-mail must also include following elements in each commercial e-mail:

- Clear identification that the message is an advertisement or solicitation.
- The sender’s valid physical postal address. This is typically the sender’s street address, but can also be post office box that the business has accurately registered with the US Postal Service or a private mailbox that the business has accurately registered with a commercial mail receiving agency established pursuant to US Postal Service regulations.

(15 U.S.C. § 7704(a)(3)-(5)(A)(i)-(iii).)

### SEXUALLY ORIENTED MATERIAL

The CAN-SPAM Act and the FTC’s related rules set out additional restrictions on initiators of commercial e-mails containing sexually oriented material. These restrictions relate to the e-mail’s:

- Subject line (see *Message Subject Line*).
- Content (see *Message Content*).

These restrictions do not apply, however, if the e-mail recipient has given prior affirmative consent to receive these messages from the sender.

The CAN-SPAM Act defines sexually oriented material as any material that “depicts sexually explicit conduct . . . unless the depiction constitutes a small and insignificant part of the whole” where the remaining content is not primarily devoted to sexual matters (15 U.S.C. § 7704(d)(4)).

### Message Subject Line

The FTC’s Adult Labeling Rule requires that the:

- Subject line of a commercial e-mail not contain any sexually oriented material.
- The phrase “SEXUALLY-EXPLICIT: “ appears in capital letters as the first 19 characters in the subject line of any commercial e-mail message that contains sexually oriented material.

(16 C.F.R. § 316.4(a).)

### Message Content

To prevent recipients from being exposed unintentionally to sexually oriented material in a commercial message, the FTC rule also limits the content that can be initially visible by a recipient using the electronic equivalent of a “brown paper wrapper.” The content of these messages must only contain:

- The phrase “SEXUALLY-EXPLICIT: “.
- The same required information as other commercial e-mails, including:
  - Clear and conspicuous identification that the message is an advertisement or solicitation.
  - Clear notice of the recipient’s ability to opt out of receiving future messages and a valid opt-out mechanism (either a functioning return e-mail address or other internet-based mechanism) that remains operational for no less than 30 days after the e-mail was sent.
  - The sender’s valid physical postal address, clearly and conspicuously displayed.
- Any necessary instructions identifying how the recipient may access the sexually oriented material. If the e-mail includes these instructions, the instructions must come after a clear and conspicuous statement that to avoid viewing the sexually oriented material, a recipient should delete the message without following the instructions.

(16 C.F.R. § 316.4(a)(2).)

## COMMON MARKETING PRACTICES: “FORWARD-TO-A-FRIEND” E-MAILS, MULTIPLE SENDERS AND AFFILIATE MARKETING

### “FORWARD-TO-A-FRIEND” E-MAILS

Marketers use a common practice to enable recipients of a commercial e-mail to forward the message (or a similar one) to one or more friends. These “Forward-to-a-Friend” e-mails are

typically sent using one of two methods:

- A web-based mechanism provided by the business that originally sent or provided the content (either in an e-mail or on a website).
- Using the consumer’s own e-mail program.

When using forward-to-a-friend e-mails as a marketing tool, a business must determine whether it is an initiator or sender of these messages under the CAN-SPAM Act (see *Who Must Comply with the CAN-SPAM Act?*). If the web-based mechanism merely provides a method for a recipient to forward the message along to a friend, or if the recipient forwards the message using a personal e-mail program, absent more, the originator is not likely the initiator of the forwarded message and is not subject to the CAN-SPAM Act. In this case, the business’s role would probably be considered solely routine conveyance. Where the recipient forwards the message using a personal e-mail program, without consideration or inducement, the business likely is not involved at all.

The FTC has clarified that a business’s use of language merely encouraging a consumer to forward a message to a friend does not, without more, subject the business to the CAN-SPAM Act’s requirements for senders of commercial e-mails (see FTC’s discussion at 73 Fed. Reg. 29654, 29671).

If the business “procures” the forwarded message, however, the business is considered to be the initiator or sender, and the commercial message must comply with the CAN-SPAM Act. A business can procure the forwarding of a message through several actions, including by either:

- Offering the recipient money, coupons, discounts, awards, additional entries in a sweepstakes or similar consideration for forwarding the message.
- Intentionally inducing the recipient to forward the message, for example, by paying a marketing affiliate (see *Affiliate Marketing*) who in turn uses sub-affiliates, to send commercial messages to drive traffic to the business’s website. Although no direct relationship between the business and the sub-affiliate exists, if the business intentionally induces the forwarding of the commercial messages through the affiliate, it is considered to be the sender.

### MULTIPLE SENDERS

The FTC rules also clarify CAN-SPAM Act requirements when a single e-mail contains commercial messages from multiple senders (73 Fed. Reg. 29654, 29655).

When multiple businesses’ products or services, or internet websites, are advertised or promoted in a single message, each business is a sender for purposes of CAN-SPAM Act compliance, unless the businesses have designated a single sender of the commercial message by complying with all of the following requirements:

- The single business meets the CAN-SPAM Act’s definition of “sender.” This is the person that both initiates the message and whose products or services, or internet websites are advertised or promoted in the message.

- The single business is identified in the “From” line as the sole sender of the message.
- The single business is in compliance with the:
  - prohibition on false or misleading transmission information;
  - prohibition on deceptive subject headings;
  - requirement to include a functioning opt out;
  - requirement to include clear and conspicuous identification that the message is an advertisement or solicitation, a clear and conspicuous notice of the opportunity to opt out, and a valid physical postal address of the sender; and
  - requirement to include warning labels on commercial e-mail that contains sexually oriented material.

(16 C.F.R. § 316.2(m)) (see also *Commercial Message Requirements* and *Sexually Oriented Material*).

In this instance, only the designated sender must comply with the CAN-SPAM Act’s requirements for senders, including the obligation to scrub against any opt-out lists maintained by the sender and honoring opt-out requests. Only the designated sender’s valid physical postal address must appear in the message. If the above requirements are not complied with, each business must comply with the CAN-SPAM Act’s requirements for senders (including the obligation to scrub against all of the senders’ opt-out lists).

Even where a single sender is designated, the other businesses will be deemed initiators of the commercial e-mail for CAN-SPAM purposes.

## AFFILIATE MARKETING

A commercial e-mail can have more than one initiator or sender (see *Who Must Comply with the CAN-SPAM Act?*). Companies often engage third-party affiliate marketers to increase traffic to the company’s website. These affiliates are typically paid based on the number of individuals who, directed by the affiliates, ultimately visit the business’s website or make a purchase on the website.

FTC has brought several claims against both companies whose product or service was advertised in the commercial e-mail as well as the affiliate that sent the message. In these situations, the company is deemed the sender of the commercial e-mail. The affiliate, who typically originates or transmits the e-mail message, is an initiator. If the affiliate also advertises its own services or products, it is also a sender under the CAN-SPAM Act and the rules concerning multiple senders apply (see *Multiple Senders*).

A company also may be liable for violations of the CAN-SPAM Act’s prohibition on false or misleading transmission information (see *Prohibition on False or Misleading Transmission Information*) by a marketing affiliate or other third party promoting the company’s business or its products or services if the company:

- Knows (or should have known) of the violations.
- Profits from the prohibited practice.
- Fails to stop or report the violations.

(15 U.S.C. § 7705(a).)

## E-MAIL SENT TO A WIRELESS DEVICE

The FCC is authorized by the CAN-SPAM Act to regulate communication to wireless devices and has enacted certain regulations addressing certain commercial messages sent to wireless devices (47 C.F.R. § 64.3100).

In contrast to the general opt-out requirements set out in the CAN-SPAM Act and FTC rules, the FCC has prohibited the sending of commercial messages to certain e-mail addresses provided by wireless carriers specifically for mobile messaging services, for example, “customer@wirelesscompany.com” (referred to as mobile service commercial messages), unless the subscriber gives express prior authorization (opts in), which can be written or oral.

Specifically, the FCC maintains a list of domain names for wireless messaging services posted on its website (<http://www.fcc.gov/cgb/policy/DomainNameDownload.html>). Wireless carriers are required to update this list periodically. Unless a recipient has given express prior authorization, a person must not initiate commercial e-mail to any address with a domain name that has been on the list for at least 30 days before the message is sent, or otherwise knowingly initiate a mobile service commercial message.

When requesting express prior authorization, an initiator of a mobile service commercial message must, among other things:

- Clearly state the identity of the entity that will be sending the messages.
- Notify the subscriber that he may be charged by the wireless carrier for receipt of these messages.
- Disclose that the subscriber can revoke his authorization at any time.

(47 C.F.R. § 64.3100(d).)

Once a recipient expressly authorizes these messages, similar to the FTC’s rules for commercial messages, any person initiating a mobile service commercial message must include:

- Clear notice of the recipient’s ability to opt out of receiving future messages from the sender of the e-mail.
- A clearly and conspicuously displayed functional return e-mail address or internet-based method for the subscriber to opt out.

A sender must stop sending further messages within 10 days after receiving an opt-out request. Like the FTC’s rules, the opt-out methods must be functional for at least 30 days after the message was sent.

In addition, the FCC rule requires that where recipients have electronically provided express prior authorization (for example, by dialing a short code) they must be able to opt-out of future e-mails by the same electronic method. The initiator of the message must also ensure that at least one opt-out option is provided that does not result in additional charges to the mobile service subscriber.

(47 C.F.R. § 64.3100(b).)

## ENFORCEMENT AND PENALTIES FOR NON-COMPLIANCE

Although the FTC is the primary enforcer of the CAN-SPAM Act, the CAN-SPAM Act also allows various federal, state and private parties to bring claims for violations. Penalties for non-compliance vary based on:

- The party bringing the claim, for example, the FTC, the FCC and other federal agencies, state attorneys general and private actions brought by internet service providers (as described in more detail below).
- Whether the violation was willful, knowing or aggravated (see also *Aggravated Violations*).

### FTC ENFORCEMENT

The FTC has authority to enforce the CAN-SPAM Act as if a violation were an unfair or deceptive act or practice prohibited under the Federal Trade Commission Act. The FTC can seek civil penalties for CAN-SPAM Act violations as if they were violations of trade regulation rules. This includes:

- Civil penalties up to \$16,000 for each separate e-mail that violates the CAN-SPAM Act (if based on actual knowledge or knowledge fairly implied).
- Injunctive relief (even without a showing of knowledge).

(15 U.S.C. § 7706(a), (d), (e).)

### ENFORCEMENT BY OTHER AGENCIES

Certain other agencies have authority under the CAN-SPAM Act to enforce it. These agencies generally regulate certain types of entities or activities outside the scope of the FTC's jurisdiction. Penalties for non-compliance are determined by the regulatory regime enforced by the specific agency (15 U.S.C. § 7706(b)). These agencies include:

- The Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation Board of Directors and the Director of the Office of Thrift Supervision under the Federal Deposit Insurance Act.
- The Board of the National Credit Union Administration, enforcing the CAN-SPAM Act under the Federal Credit Union Act.
- The Securities and Exchange Commission, enforcing the CAN-SPAM Act under the Securities Exchange Act of 1934, the Investment Company Act of 1940 and the Investment Advisors Act of 1940.
- State insurance authorities, enforcing the CAN-SPAM Act under state insurance laws.
- The Secretary of Transportation, enforcing the CAN-SPAM Act under the US Code's air commerce and safety provisions (49 U.S.C. §§ 40101-40129).
- The Secretary of Agriculture, enforcing the CAN-SPAM Act under the Farm Credit Act of 1971.
- The FCC, enforcing the CAN-SPAM Act under the Communications Act of 1934.

### STATE ENFORCEMENT

The CAN-SPAM Act authorizes state attorneys general, officials and other agencies to bring claims for CAN-SPAM Act violations against residents of that state. These state agencies can seek:

- Injunctive relief.
- Damages for actual loss or statutory damages up to \$250 per violation, whichever is greater, with a maximum award of \$2,000,000. Each separately addressed unlawful message is treated as a separate violation. Notably, claims for false or misleading headers (see *Prohibition on False or Misleading Subject Headers*) are not limited by this cap.
- Three times the amount of statutory damages for willful, knowing or aggravated violations (see also *Aggravated Violations*).
- Costs of bringing the action and reasonable attorney fees.

(15 U.S.C. § 7706(f).)

### INTERNET SERVICE PROVIDER CLAIMS

Internet service providers (ISPs) are authorized to bring claims under the CAN-SPAM Act for certain violations (for example, violations of the prohibition on false or misleading transmission information or the requirement to place warning labels for sexually oriented material) and may seek:

- Injunctive relief.
- Actual damages or statutory damages for false or misleading headers up to \$100 per violation, whichever is greater, with no limitation on the maximum award.
- For all other violations, actual damages or statutory damages of up to \$25 per violation, whichever is greater, with a maximum award of \$1,000,000.
- Three times the amount of statutory damages for willful, knowing or aggravated violations (see also *Aggravated Violations*).
- Costs of bringing the action and reasonable attorneys' fees.

Each separately addressed unlawful message is treated as a separate violation. Where an ISP is bringing a claim, the term "procure" for purposes of initiating a commercial e-mail message ((see *Who Must Comply with the CAN-SPAM Act?*) requires that the person providing consideration or inducing another person to initiate the e-mail transmission has actual knowledge, or should have known, that the person transmitting the e-mail is engaging, or will engage, in a pattern of practice violating the CAN-SPAM Act.

(15 U.S.C. § 7706(g).)

### FCC CLAIMS

The CAN-SPAM Act authorizes the FCC to bring claims for violations of its rule regarding the sending of commercial e-mail to wireless devices (see *E-mail Sent to a Wireless Device*). If the action is brought against a telecommunications provider (a common carrier), the FCC can seek up to \$150,000 per

violation with a maximum of \$1,500,000 per incident. If the action is brought against a marketer who is generally not a common carrier and therefore not subject to FCC jurisdiction, the FCC may first issue a citation. If additional claims are brought against a marketer that previously received a citation, the FCC can seek fines up to \$16,000 per violation with a maximum of \$112,500 per incident.

The FCC can also bring claims for other violations of the CAN-SPAM Act (not just for commercial e-mails sent to wireless devices) against entities subject to its jurisdiction, for example, telecommunications providers or marketers advertising telecommunications products (see *Enforcement by Other Agencies*).

## VIOLATIONS RELATING TO SEXUALLY ORIENTED MATERIAL

Knowing violations of the CAN-SPAM Act's restrictions on commercial e-mails containing sexually oriented material includes fines and imprisonment of up to five years (15 U.S.C. § 7704(d)(5)).

## OTHER CRIMINAL PENALTIES

In addition to criminal penalties associated with knowing violations of the rules for commercial e-mails containing sexually oriented material (see *Sexually Oriented Material*), the CAN-SPAM Act also carries criminal penalties for fraud and related activities.

Enforced by the Department of Justice and state attorneys general, violations subject to criminal penalties include:

- Accessing a computer without authorization and using it to intentionally initiate multiple commercial e-mail messages.
- Relaying or transmitting multiple commercial e-mail messages intending to deceive or mislead recipients or an ISP about the messages' origin.
- Materially falsifying header information in multiple commercial e-mails and intentionally initiating these messages' transmission.
- Using materially false identifying information to register for five or more e-mail accounts or two or more domain names, and intentionally initiating multiple commercial e-mail messages from any combination of these accounts or domain names.
- Falsely representing oneself as the registrant of five or more Internet Protocol addresses and intentionally initiating the transmission of multiple commercial e-mail messages from those addresses.

Criminal penalties may include:

- Fines.
- Forfeiture of assets.
- Imprisonment up to five years.

(18 U.S.C. § 1037.)

## AGGRAVATED VIOLATIONS

The following four specific practices are aggravated violations under the CAN-SPAM Act:

- **Address Harvesting.** The automatic capturing of e-mail addresses posted to websites including social networking sites, blogs, newsgroups, message boards and chat rooms.
- **Dictionary Attacks.** The automated process of creating possible name combinations that may be valid e-mail addresses.
- **Spoofing.** The relay or retransmission of e-mail messages through another computer that is accessed without authorization.
- **Automated Creation of Multiple E-mail Accounts.** The automatic creation of a large number of e-mail accounts so that those accounts may be used to send commercial e-mail.

While these are not considered separate violations, if a party commits an aggravated violation along with a violation of the requirements for commercial messages or sexually oriented material (see *Commercial Message Requirements* and *Sexually Oriented Material*), the party may be liable for enhanced statutory damages of up to three times the damages.

(15 U.S.C. § 7704(b).)

## PREEMPTION AND REMAINING CAUSES OF ACTION

The federal CAN-SPAM Act preempts any state laws expressly regulating commercial e-mail messages, except to the extent that these laws generally prohibit false or deceptive acts or practices (such as states' general consumer protection laws) (15 U.S.C. § 7707(b)(1)).

Although state laws generally are preempted by the CAN-SPAM Act, Congress has attempted to create a balance by permitting state attorneys general to bring claims under the CAN-SPAM Act for violations affecting residents in their states (see *Enforcement and Penalties for Non-compliance*).

Additionally, the CAN-SPAM Act expressly does not preempt state laws that are

- Not specific to e-mail, including trespass, contract, or tort law.
- Related to fraudulent or deceptive acts or computer crimes.

(15 U.S.C. § 7707(b)(2).)

## BEST PRACTICES FOR E-MAIL MARKETING

Practical tips for CAN-SPAM Act compliance are set out below.

### REQUIREMENTS FOR ALL COMMERCIAL MESSAGES

#### The Mailing List

- The mailing list should include only persons who have affirmatively agreed (opted in) to receive commercial e-mail from the business. While this is not a legal requirement under the CAN-SPAM Act, it is an industry best practice.
- The mailing list must not include any recipient who has previously asked not to receive commercial e-mail from the business (opted out).
- Scrub the mailing list against the business's "do not e-mail" list at the last possible, commercially reasonable moment before the e-mail is sent.

#### The E-mail Message

- The message must include complete and accurate transmission and header information.
- The "From" line must identify the business as the sender. This does not have to include the business's formal name. For example, it may contain the business's name, trade name or product or service name. The key requirement is that the "From" line provide the recipient with enough information to understand who is sending the message.
- The "Subject" line must accurately describe the message's content.
- The message must clearly include the business's valid, current physical postal address. This address can be a:
  - street address;
  - post office box that the business has accurately registered with the US Postal Service; or
  - private mailbox that the business has accurately registered with a commercial mail receiving agency established pursuant to US Postal Service regulations.
- The message must disclose that it is an advertisement or solicitation unless the e-mail message is sent only to recipients who have affirmatively agreed (opted in) to receive these messages from the business.

#### The Opt-out Mechanism

- The message must clearly explain that the recipient may opt out of receiving future commercial messages from the business.
- The message must include either an e-mail address or other online mechanism that the recipient may use for this opt out. The mechanism must not require the recipient to:

- do anything more than reply to the e-mail or visit a single web page to opt out;
- make any payment or submit any personal information, including account information (other than e-mail address), to opt out; and

The opt-out mechanism must work for at least 30 days after the e-mail is sent.

- Ensure that the explanation of how a recipient can opt out is easy to read and understand.
- The business may include a menu of opt-out options that permit the recipient to select the types of commercial messages the recipient would like to continue receiving. However, one option must permit opting out of all commercial messages from the business.
- Honor all opt-out requests within ten business days.
- Opt-out requests do not expire. An opt-out is overridden only by the recipient's subsequent express (opt in) request to receive commercial e-mail.
- Do not sell, share or use the business's opt-out list for any reason other than to comply with the law.

#### Monitoring Opt-out Capabilities

The business should implement procedures to ensure that its opt-out capabilities actually work. An example of a basic procedure to test the opt-out procedure is as follows:

- Establish e-mail accounts with several major private e-mail account providers (for example, Gmail, Yahoo, Hotmail, AOL, and so on) and add these e-mail addresses to the business's mailing list.
- For each e-mail address created for monitoring purposes, use the business's opt-out mechanism to remove the e-mail address from the mailing list.
- Repeat this procedure on a regular basis (for example, at least every two weeks).
- Examine the e-mail received by the monitoring e-mail account to confirm that the:
  - opt-out mechanism works;
  - opt-out request is honored within 10 business days; and
  - monitoring e-mail account no longer receives commercial messages from the business.
- If the monitoring and testing process reveals problems, the business should immediately fix the issues.

#### Third-party Marketing Affiliates or Service Providers

When using third-party service providers, including affiliate marketers:



## BEST PRACTICES FOR E-MAIL MARKETING (CONTINUED)

- Ensure that the written contract with the service provider clearly sets out each party's responsibilities for compliance with the CAN-SPAM Act and includes appropriate and adequate remedies for non-compliance.
- Monitor their compliance with the CAN-SPAM Act. Both the company whose product or service is advertised as well as the individual or entity sending the message are potentially liable for violations of the CAN-SPAM Act.

## ADDITIONAL REQUIREMENTS FOR MESSAGES SENT TO WIRELESS DEVICES

When sending commercial messages to wireless devices:

- Ensure that you have the recipient's prior, affirmative consent (opt in) to send the commercial message. The consent can be oral, written or electronic.
- Ask for consent in a way that involves no cost to the recipient, for example:
  - do not send the request to the wireless device; and
  - allow the recipient to respond in a way that involves no cost (such as an online, e-mail or postal mail sign-up).
- When seeking consent, make it clear that the recipient:
  - is agreeing to receive commercial e-mail on his wireless device;
  - may be charged to receive the e-mail; and
  - can revoke his consent at any time.

**Practical Law Company** provides practical legal know-how for law firms, law departments and law schools. Our online resources help lawyers practice efficiently, get up to speed quickly and spend more time on the work that matters most. This Article is just one example of the many resources Practical Law Company offers. Discover for yourself what the world's leading law firms and law departments use to enhance their practices.

## Contact Us

**Practical Law Company**  
**747 Third Avenue, 36th Floor**  
**New York, NY 10017**  
**646.562.3405**  
[plcinfo@practicallaw.com](mailto:plcinfo@practicallaw.com)  
[www.practicallaw.com](http://www.practicallaw.com)