The CAN-SPAM Act of 2003: Overview and Analysis

By Stephen H. LaCount, Esq.

Congress has passed the long-awaited legislation that establishes federal regulation of spam email. The bill, known as the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (or "CAN-SPAM Act"), preempts many provisions of existing state anti-spam laws, including the highly restrictive California law that was set to take effect on January 1, 2004. Inasmuch as CAN-SPAM is scheduled to take effect on January 1, 2004, businesses that utilize email in their advertising and communication channels must move quickly to study the CAN-SPAM Act and implement compliance programs that meet its requirements.

The new Act contains a complex set of prohibitions and definitions, some of which are ambiguous and subject to further clarification by the Federal Trade Commission ("FTC"). This alert will summarize the principal provisions of the Act and analyze areas of uncertainty which may pose complications for businesses bringing their email practices into compliance with the Act.

Key Provisions of the Can-Spam Act

E-Mail Advertising is Permitted. Unlike the highly restrictive California statute that was set to take effect in January 2004, the CAN-SPAM Act allows companies to send email advertisements to potential customers where the recipients have not given prior consent to such mailings (or where the sender does not enjoy a preexisting or current business relationship).

CAN-SPAM Applies to Commercial Electronic Mail Messages. The Act applies to any "commercial electronic mail message" – defined as "any electronic mail message the *primary purpose* of which is the commercial advertisement or promotion of a commercial product or service." [emphasis added].

Recipients Must Be Allowed to Opt Out. All commercial electronic mail messages [also referred to below as "CEMMs"] must give recipients the means to "opt out" from receiving future e-mails from the sender. Specifically, the email must give the recipient the ability to send a reply electronic mail message or other form of Internet-based communication that affirmatively notifies the sender that the recipient does not wish to receive further emails. Also, the recipient's ability to make an opt-out response must be maintained by the sender for at least 30 days after the original message is transmitted. It should also be noted that the opt-out requirements of the Act include additional refinements. For example, the recipient may be provided with a list or menu which allows a choice between types of commercial electronic mail messages which may be received from the sender, provided that the list or menu includes the option to opt-out of *all* CEMMs from the sender.

Email Ads Must Not Be Sent to Recipients Requesting Not to Receive Them. If the recipient has exercised the opt-out option, the sender must honor that request and *cease transmission of emails ads to that recipient within 10 business days from the date of the receipt of the opt out request*. The sender (or any other person who is aware of the opt-out request) is also prohibited from selling, leasing, exchanging or transferring the email addresses of persons who have opted out – except in the case where the recipient has given express consent.

Most of the Act's Prohibitions Do Not Apply to Transactional or Relationship Emails. Commercial electronic mail messages regulated by the CAN-SPAM Act do not include "transactional or relationship message[s]" – defined as "email message[s] the primary purpose of which is – (i) to facilitate, complete or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; (ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient; (iii) to provide [notifications of changes in product or service terms or features, notifications of changes to recipient's standing or status, or regular periodic account balance statements and information with respect to subscriptions, memberships, accounts, loans or comparable ongoing commercial relationships involving a recipient's purchase or use of products or services offered by the sender]; (iv) to provide information directly related to employment relationship or related employment plan in which recipient is currently involved, participating, or enrolled, or (v) to deliver goods or services, including product updates, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender." *Please note that this is not the same broad exemption, common in state anti-spam laws, permitting businesses to contact their past and present customers without observing the restrictions applicable to emails sent to strangers.* The Act authorizes the FTC to modify the definition of "transactional or relationship message" as needed to take into account changes in technology and email practice.

Misleading Headers Must Not Mask the Origin of Email Ads. The CAN-SPAM Act broadly prohibits practices which attempt to conceal the origins of email ads or the identities of their senders. In particular, the Act prohibits falsification of header information, false registrations for email accounts or IP addresses used in connection with CEMMs, and the retransmission of such emails for the purpose of concealing origin.

Commercial Emails Must Be Identified as Such. Email advertisers are required to identify their messages as advertisements or solicitations by means that are "clear and conspicuous"-unless the recipient has given "prior written consent" to the receipt of the message. It should be noted that the Act also requires a special subject heading, to be specified by the FTC, for any CEMM that includes sexually oriented material.

Most Provisions of State Anti Spam Laws Are Preempted. One of the most important provisions of the CAN-SPAM Act deals with preemption. Specifically, the Act "supercedes any statute, regulations, or rule of a state or political subdivision of a state that expressly regulates the use of electronic email to send commercial messages, except to the extent that such statute, regulation or rule prohibits falsity or deception in any portion of a CEMM or information attached thereto." In effect, by preempting state anti-spam restrictions not related to fraud or deception, the new Act protects legitimate businesses from more restrictive state regulation such as that envisioned by California's anti-spam law.

Recipients Generally Do Not Have the Right to Sue Spammers. Unlike the pending California statute and some other state anti-spam laws, CAN-SPAM does not permit recipients to sue spam senders for violations. Enforcement will be in hands of the FTC or state law enforcement authorities. Pursuant to its enforcement authority, the FTC may investigate, impose monetary penalties, enter into consent decrees, or refer violations to the Department of Justice for criminal prosecution. States may bring actions seeking injunctive relief or an award of damages equal to the actual monetary loss, or statutory damages. As discussed below, certain kinds of conduct – referred to in the Act as "aggravated violations" will incur heightened penalties.

Internet Service Providers("ISPs") Do Have the Right to Sue Spammers. The CAN-SPAM Act grants ISPs the right to bring civil lawsuits against violators if they have been adversely effected (i) by use of false or misleading information transmission, or (ii) by one of the defined aggravating violations [see discussion below], or (iii) by a pattern or practice that violates the Act's opt-out provisions, or (iv) by a failure to comply with the requirements concerning sexually oriented materials. ISPs which succeed in court may recover the greater of the actual monetary or statutory damages. However, if willful or knowing or aggravated conduct is present, an ISP plaintiff may recover up to three times this amount.

Areas of Uncertainty and Related Compliance Issues

Future Clarification and Regulatory Proceedings By the FTC.

The Act delegates a series of future studies, reports, and rulemaking activities to the FTC, including the task of defining certain key terms – or refining those already provided in the Act. In particular, the FTC has been given the responsibility of defining when an email's "primary purchase" is the promotion or advertisement of a commercial product or service, key elements in the classification of CEMMs. *It should also be noted that the Act provides no guidance to determine whether a message that does not directly advertise a product or service is nonetheless a "promotion" of a product or service.*

In addition, the FTC is tasked to promulgate other regulations and recommendations in the next couple of years. Examples include prescribing warning labels for CEMMs containing sexually oriented material; drawing up a plan and timetable for establishing a nationwide "Do Not E-Mail" registry, and developing a standard to include identifiers in CEMM subject lines (such as the use of "ADV" or other similar identifiers). These post-enactment legislative mandates guaranty that the FTC will play a primary role in the evolving federal regulation of commercial email advertisements and promotions.

Opt Out Requirements and Responsibility of Parties in the Email Transmission Chain.

The Act makes it unlawful to "initiate the transmission to a protected computer of any commercial electronic mail message that does not contain a functioning return electronic mail address or other internet based mechanism, clearly and conspicuously displayed," that a recipient may use to request "not to receive future commercial electronic mail messages from that sender

at the electronic mail address where the message was received…" ("Protected Computer", a term borrowed from the federal Computer Fraud and Abuse Act, is defined in that statute to include any computer connected to the public internet). This opt-out mechanism necessarily involves three parties: (1) the recipient of the message; (2) the sender – defined by the Act as a "person who initiates a commercial electronic email message and whose product, service, or Internet web site is advertised or promoted by the message"; and (3) the initiator – defined as the party which "originate[s] or transmit[s] or procure[s] the origination or transmission of such message, but [it does] not include actions that constitute routine conveyance of such message."

In short, with the exception of the exemption accorded by the Act to Internet service providers, email providers, and other entities that process the automatic transmission and routing of emails ("routine conveyors"), all participants in the process that results in the sending of a CEMM (e.g., vendors of email advertising services, email address list providers, suppliers of goods and services) may be responsible for compliance with the opt-out requirements and other provisions of the CAN-SPAM Act. As companies have only ten business days to comply with opt-out requests, it will be important to centralize marketing distribution lists and opt-out request information to ensure timely compliance. In addition, compliance with the Act must extend to individual CEMMs sent by salespeople, marketing staff and other employees – a significant risk factor to be addressed in a company's internal compliance education program.

Aggravated Violations and Criminal Anti-Fraud Provisions.

Certain types of conduct – defined in the Act as "aggravated violations" – will incur more severe penalties. Specifically, penalties may be increased for violations accompanied by any of the following: (i) initiating or assisting in the initiation of a commercial electronic mail message with actual or constructive knowledge that the recipient's email address was obtained by an automated process from an online site with a posted policy of not giving out addresses for purposes of third party mailings, or was obtained by the use of a program for random generation of email addresses; (ii) use of scripts or other automated means to register for multiple email accounts or online user accounts from which to transmit an unlawful email message; and (iii) relaying or retransmitting an unlawful email message from a protected computer or computer network that was accessed without authorization. This definitional framework has broad sweep and means, for example, that initiators are liable for aggravated violations when they know, or should have known, that a CEMM was transmitted to addresses improperly obtained by "scraping" from websites or online services.

Several provisions of the Act are designed to control the use of email to mislead recipients. Some provisions apply to transmission of multiple CEMMs; others apply to the transmission of a single CEMM. Still others apply to transactional or relationship messages. Certain of these anti-fraud provisions – especially those applicable to multiple emails and methods used by spammers to obscure the origin of their messages – are defined by amendments to the chapter of the U.S. Criminal Code and carry criminal penalties. Examples of prohibited spammer methods include (i) routing spam messages through computers (other than through the originating computer) by hacking or other means, (ii) materially falsifying header information and the intentional transmission of such messages, (iii) use of email accounts and domain names which have been registered through the use of falsified registration information, and (iv) registration under a false identity for 5 or more email or online user accounts or 2 or more domain names and intentionally

initiating multiple CEMMs from any combination of such accounts or domain names. Specific criminal penalties include fines and imprisonment for up to 3 years. The imprisonment term may be extended up to 5 years if the defendant has been previously convicted of one of the multiple-CEMM fraud offenses, the federal Computer Fraud and Abuse Act or the law of any state for similar conduct.

As previously mentioned, certain anti-fraud provisions of the Act apply to transactional and relationship messages. Specifically, such messages may not be sent if the message contains, or is accompanied by, "header information that is materially false or materially misleading." As stated in the Act, this includes header information that is "technically accurate" but may include an originating email address, domain name or Internet protocol address that was obtained by false or fraudulent pretenses.

Application to Mobile Service Messages. The prohibitions of the Act do not immediately apply to commercial email messages sent to subscribers of mobile services such as cellular phone users. However, the Act requires the Federal Communications Commission, in consultation with the Federal Trade Commission, to establish rules to protect consumers from unwanted mobile commercial service messages within 270 days of enactment.

Conclusion

The CAN-SPAM Act is the foundation of a new federal regime to regulate spam email and represents a significant advance in the standardization of anti-spam laws in the United States. Not surprisingly, given the subject matter and broad reach of the statute, the Act poses some complexities and definitional issues which may be not be clarified or resolved for some months or years. However, businesses which sell or market products or services using commercial electronic mail messages should not delay taking prompt action to comply (the CAN-SPAM Act takes effect on January 1, 2004).