

The DMA's Analysis of 'Can Spam Act of 2003'

December 11, 2003 – The following is a Direct Marketing Association analysis of the "Can Spam Act of 2003" (S. 877), which Congress sent to the President for signing on December 8, 2003. President Bush is expected to sign the measure, which would take effect on January 1, 2004.

The following analysis was prepared by The DMA with consultation from its outside legal counsel, Piper Rudnick, a Washington, DC law firm.

* * *

Congress has passed legislation governing the sending of commercial electronic mail advertisements and promotions. President Bush is expected to quickly signature for final enactment, which is expected shortly.

The measure will cover all commercial e-mail solicitations – i.e., not just those messages sent that are unsolicited (where there is no established customer relationship and a marketer is looking for new business).

It is of major significance that this new federal anti-spam law will pre-empt all of the numerous state laws that have been passed in recent years regulating commercial e-mail.

The effective date of S. 877 (The Can Spam Act) is January 1, 2004, which means it will also pre-empt the California "opt-in" law that otherwise would have taken effect on that date. The new federal law will preserve state laws "to the extent that" they prohibit falsity or deception in commercial e-mail, as well as state common law rules.

Requirements for Transmission of Messages

The new law will require that all e-mail – including business-to-consumer and business-to-business – for which the primary purpose is the commercial advertisement or promotion of a commercial product or service must include:

- Clear and conspicuous notice of the opportunity to decline to receive further commercial e-mail messages from the sender.
- A functioning return e-mail address or other Internet-based mechanism that is clearly and conspicuously displayed that recipients can use to request not to receive future advertisements or promotions. This return address or other mechanism must be capable of receiving such messages for at least 30 days after the transmission of the original message. The sender of the message may not send subsequent advertisements or promotions more than 10 business days after the request from any recipient to be removed from future commercial e-mail communications. If the recipient has requested not to receive further advertisements or promotions, the

sender may not request, sell, lease, exchange, or otherwise transfer or release the e-mail address of the recipient.

- Clear and conspicuous identification that the e-mail is an advertisement or solicitation. The sender of the e-mail is responsible for determining how to indicate that the message is a solicitation (i.e., there is no requirement to include any specific language, such as, “this is an advertisement,” or any labeling, such as “ADV” in the subject line). However, if the recipient has provided affirmative consent to receive the message, then this identification is not required.
- A valid physical postal address of the sender. A post-office box (PO Box) or mail-drop does not suffice. The physical address must be somewhere that a consumer can physically find you and/or your employees.

These requirements on commercial e-mail will not apply to “transactional or relationship” e-mail messages, such as e-mail about account balances, memberships, subscriptions, or other ongoing commercial relationships that are not primarily solicitations.

Sexually Oriented Warning Labels

The new law will require senders of commercial e-mail that includes sexually oriented material to:

- Include in the subject heading initially viewable specific marks or notices to ensure that when the message is opened, it includes **only** the mark or notice indicating that the message is sexually oriented (i.e., e-mails must never open immediately to sexually explicit material);
- The other required opt-out and standard inclusions as outlined previously; and
- Instructions on how to access the sexually oriented material.

The marks or notices will be determined by the Federal Trade Commission (FTC) in the coming months.

New Civil Provisions

The federal anti-spam legislation contains civil prohibitions against:

- The sending of false or misleading header or transmission information in a commercial e-mail message;
- Using deceptive subject headings;

- Using another computer to relay or retransmit commercial e-mail for the purpose of disguising the commercial e-mail's origin;
- Sending commercial e-mail that includes an originating e-mail address, domain name, or Internet protocol address that was obtained by means of false pretenses or representations.

The law will provide additional remedies against those who violate the falsification and deception provisions ("aggravated violations") by "harvesting" e-mail addresses or engaging in "dictionary attacks."

Harvesting is the practice of collecting, through an automated means, e-mail addresses that are posted on websites or online services.

Dictionary attacks occur when e-mail addresses are generated by combining names, letters, or numbers into numerous permutations in the hope of generating functioning e-mail addresses.

Aggravated violations also exist for the automated creation of multiple e-mail accounts to transmit otherwise unlawful messages and the relay or retransmission of commercial e-mail from computers that have been accessed without authorization.

***Businesses Knowingly Promoted by Electronic Mail
with False or Misleading Transmission Information***

The law also will make it unlawful for a business to promote goods and services in a commercial e-mail message sent by others that the business knows violate provisions of the law.

Strong New Criminal Enforcement Tools

The law will criminalize egregious spammer tactics. These include:

- New prohibitions against commercial e-mail involving hacking into someone else's computer to send bulk spam;
- Using "open relays" to send multiple spam with the intent to deceive ISPs or recipients as to the origin of the messages;
- Falsifying header information in commercial e-mail;
- Registering for five or more e-mail accounts or two or more domain names using false information and then sending multiple spam from those accounts;
- Falsely representing oneself to be the holder of five or more Internet protocol addresses and sending multiple commercial e-mail messages from such addresses.

Ordinary violations will be misdemeanors.

Violations involving hacking, larger numbers of commercial e-mail messages or falsified registration, or loss or gain aggregating more than \$5,000 in a year, or a criminal spam organization are punishable by a three-year felony.

Five-year felony penalties are available for violations undertaken in furtherance of another felony and violations by someone with a prior offense involving hacking or criminal spam under federal or state law.

Do-Not-E-mail Registry

The FTC is required to set forth a plan and timetable for establishing a nationwide marketing do-not-e-mail registry that includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the FTC has regarding such a registry. The FTC has the authority, but is not required, to implement a registry; it will determine over the next six months whether to adopt one.

Wireless E-mail

The law will require the Federal Communications Commission (FCC) to issue rules to “protect consumers from unwanted mobile service communications,” including text-messages. Mobile commercial messages are messages that are transmitted directly to a wireless device.

The law will require the FCC to define rules that will enable subscribers to commercial mobile services to avoid receiving mobile service commercial messages.

The law will require that the FCC consider whether to require providers of commercial mobile services to allow subscribers to indicate a desire not to receive future mobile service commercial messages at the time of subscribing to such service.

The DMA’s ‘Anti-Spam Working Strategy’

In order to protect your business and ensure that it grows in the ever-evolving e-mail marketplace, The DMA also recommends that you continue to abide by the tenets of the anti-spam working strategy – which in some cases goes above and beyond the legal requirements set forth in the Can Spam Act – and will help distinguish your business as a profitable and ethical marketer.

**Direct Marketing Association
Anti-Spam Working Strategy ***

The DMA is committed to upholding the principles outlined in this working document in its continuing efforts to combat spam while protecting legitimate e-mail marketing as an emerging and promising marketing channel.

1. **ADHERENCE TO THE FOUR PILLARS OF RESPONSIBLE E-MAIL MARKETING**

- A. An honest subject line.
- B. No forging of headers or technological deceptions.
- C. Identity of the sender, which includes a “physical” address.
- D. An opt-out that works and is easy to find and easy to use.

2. **NO HARVESTING** – No surreptitious acquisition of e-mail addresses via automated mechanisms (such as robots or spiders) without the consumer/customer’s informed consent. This includes a prohibition on dictionary attacks or other mechanisms for fabricating e-mail addresses without the awareness and prior approval of the addressee.

3. **UNIVERSAL OPT-OUT** – All commercial e-mailed communications (except for billing messages) must include a clear and conspicuous opt-out. A clear, conspicuous and ubiquitous symbol would increase awareness of the consumer’s right to opt-out . The user would be encouraged to print out a copy of the screen including this information and save it for possible prosecution if additional e-mails are received after a legislatively mandated grace period.

4. **THE GOLD LIST** – Companies agreeing to adhere to principles 1 – 3 would sign an affidavit to that effect and post a bond of, at minimum, \$500 per corporate entity. A violation of the principles would result in forfeiture of the bond. In addition, a \$100 annual fee would be paid for participating in the Gold List program. These monies would be used for enforcement as indicated below. [*See point 6 below.*] The Gold List would be provided on a weekly basis to all participating ISP’s.

5. **FEDERAL LEGISLATION** – The DMA supports Federal legislation that provides appropriate penalties for violation of the principles 1 – 3. In addition, legislation should preempt state anti-spam laws and provide for both civil and criminal penalties.

6. **ENFORCEMENT** – Significant energy must be focused on enforcing existing fraud laws as well as the Federal law described above. [*See point 5 above.*] Law enforcement agencies in the U.S. (at the Federal and state level) in other countries and global law enforcement organizations would be encouraged to focus additional resources in this area. In addition, an industry-financed group would be formed to provide professional investigation and prosecutorial resources entirely focused on the spam problem. This so-called “Silver Platter Program” would provide federal law enforcement agencies with adequate information to carry forward appropriate prosecutions. The effort would be funded by The DMA, company donations, and the Gold List fees.

* As of August 6, 2003

###