Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

Introduction

Under Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM or Act)[1], the Federal Trade Commission (FTC) is charged with issuing regulations for implementing CAN-SPAM.[2] The FTC has issued regulations, effective as of March 28, 2005, that provide criteria to determine the primary purpose of electronic mail (e-mail) messages. The FTC has also issued regulations that contain criteria pertaining to warning labels on sexually oriented materials, which became effective as of May 19, 2004.

The goals of the act are to:

- Reduce spam and unsolicited pornography by prohibiting senders of unsolicited commercial e-mail messages from disguising the source and content of their messages.
- Give consumers the choice to cease receiving a sender's unsolicited commercial e-mail messages.

Compliance authority was expressly granted to the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Office of Thrift Supervision to be enforced under Section 8 of the Federal Deposit Insurance Act. The National Credit Union Association was granted authority through the Federal Credit Union Act 12 USC 1751.

The FTC has researched and determined that a "Do Not Spam" registry (similar to the highly effective "Do Not Call" registry) would not be effective or practicable at this time.

Key Definitions

"Affirmative Consent" (usage: commercial e-mail messages)

- The recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and
- If the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's e-mail address could be transferred to such other party for the purpose of initiating commercial e-mail messages.

"Commercial E-mail Message" Any e-mail message the primary purpose of which is to advertise or promote for a commercial purpose, a commercial product or service (including content on the Internet). An e-mail message would not be considered to be a commercial e-mail message solely because such message includes a reference to a commercial entity that serves to identify the sender or a reference or link to an Internet Web site operated for a commercial purpose.

"Dictionary Attacks" Obtaining e-mail addresses by using an automated means that generates possible e-mail addresses by combining names, letters, or numbers into numerous permutations.

"Harvesting" Obtaining e-mail addresses using an automated means from an Internet Web site or proprietary online service operated by another person, where such service/person, at the time the address was obtained, had provided a notice stating that the operator of such Web site or online service would not give, sell, or otherwise transfer electronic addresses.

"Header Information" The source, destination, and routing information attached to the beginning of an e-mail message, including the originating domain name and originating e-mail address.

"Hijacking" The use of automated means to register for multiple e-mail accounts or online user accounts from which to transmit, or enable another person to transmit, a commercial e-mail message that is unlawful.

"Initiate" To originate, transmit or to procure the origination or transmission of such message but shall not include actions that constitute routine conveyance. For purposes of the Act, more than one person may be considered to have initiated the same message.

"Primary Purpose" The FTC's regulations provide further clarification regarding determination of whether an e-mail message has "commercial" promotion as its primary purpose. [16 CFR 316.3]

(1) The primary purpose of an e-mail message will be deemed to be commercial if it contains only the commercial advertisement or promotion of a commercial product or service (commercial content);

(2) The primary purpose of an e-mail message will be deemed to be commercial if it contains both commercial content and "transactional or relationship" content (***see*** below for definition) if either:

- a recipient reasonably interpreting the subject line of the e-mail message would likely conclude that the message contains commercial content; or

1 15 USC 7701–7713

2 Final rules relating to the established criteria for determining when the primary purpose of an e-mail message is commercial were published in the Federal Register on January 19, 2005 (70 FR 3110). Final rules relating to governing the labeling of commercial e-mail containing sexually oriented material was published in the Federal Register on April 19, 2004 (69 FR 21024).

- the e-mail message's "transactional or relationship" content does not appear in whole or substantial part at the beginning of the body of the message.

(3) The primary purpose of an e-mail message will be deemed to be commercial if it contains both commercial content as well as content that is not transactional or relationship content if a recipient reasonably interpreting either:

- the subject line of the e-mail message would likely conclude that the message contains commercial content; or
- the body of the message would likely conclude that the primary purpose of the message is commercial.

(4) The primary purpose of an e-mail message will be deemed to be transactional or relationship (non-commercial) if it contains only "transactional or relationship" content.

"Protected Computer" A computer:

- Exclusively for the use of a financial institution or the United States government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States government and the conduct constituting the offense affects that use by or for the financial institution or the government; or
- Which is used in interstate or foreign commerce or communication.

"Recipient" An authorized user of the electronic mail address to which the message was sent or delivered.

"Sender" A person who initiates an e-mail message and whose product, service, or Internet Web site is advertised or promoted by the message.

"Sexually Oriented Material" Any material that depicts sexually explicit conduct unless the depiction constitutes a small and insignificant part of the whole.

"Transactional or Relationship E-mail Message" An e-mail message with the primary purpose of facilitating, completing or confirming a commercial transaction that the recipient had previously agreed to enter into; to provide warranty, product recall, or safety or security information; or subscription, membership, account, loan, or other information relating to an ongoing purchase or use.

General Requirements of the CAN-SPAM Statute:

- Prohibits the use of false or misleading transmission information [§7704(a)(1)] such as:
  - False or misleading header information;
  - A "from" line that does not accurately identify any person who initiated the message; and
  - Inaccurate or misleading identification of a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.
- Prohibits the use of deceptive subject headings. [§7704(a)(2)]
- Requires a functioning e-mail return address or other Internet-based response mechanism. [§7704(a)(3)]
- Requires that commercial e-mail messages be discontinued within 10 business days after receipt of opt-out notification from recipient. [§7704(a)(4)]
- Requires a clear and conspicuous identification that the message is an advertisement or solicitation; clear and conspicuous notice of the opportunity to decline to receive further commercial e-mail messages from the sender; and a valid physical postal address of the sender. [§7704(a)(5)]
- Prohibits address harvesting (obtaining e-mail addresses using an automated means from an Internet Web site or proprietary online service operated by another person, where such service/person, at the time the address was obtained, had provided a notice stating that the operator of such Web site or online service will not give, sell, or otherwise transfer electronic addresses) and dictionary attacks (obtaining e-mail addresses by using an automated means that generates possible e-mail addresses by combining names, letters, or numbers into numerous permutations). [§7704(b)(1)]
- Prohibits hijacking, the use of automated means to register for multiple e-mail accounts or online user accounts from which to transmit, or enable another person to transmit, a commercial e-mail message that is unlawful. [§7704(b)(2)]
- Prohibits any person from knowingly relaying or retransmitting a commercial e-mail message that is unlawful. [§7704(b)(3)]
- Requires warning labels (in the subject line and within the message body) on commercial e-mail messages containing sexually oriented material. [§7704(d)]
- Prohibits a person from promoting, or allowing the promotion of, that person's trade or business, or goods, products, property, or services in an unlawful commercial e-mail message. [§7705)(a)]

Examination Objectives:

1. Assess the quality of a financial institution's compliance program for implementing CAN-SPAM by reviewing the appropriate policies and procedures and other internal controls.
2. Determine the reliance that can be placed on a financial institution's audit or compliance review in monitoring the institution's compliance with CAN-SPAM.
3. Determine a financial institution's compliance with CAN-SPAM.

4. Initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

Examination Procedures

Initial Procedures

1. Through discussions with appropriate management officials, determine whether or not management has considered the applicability of CAN-SPAM and what, if any, steps have been taken to ensure current and future compliance.
2. Through discussions with appropriate management officials, ascertain whether the financial institution is subject to CAN-SPAM by determining whether the financial institution initiates e-mail messages whose primary purpose is "commercial."

Stop here if the financial institution does not initiate "commercial" electronic mail. The financial institution is not subject to CAN-SPAM, and no further examination for CAN-SPAM is necessary.

3. Determine, through a review of available information, whether the financial institution's internal controls are adequate to ensure compliance with CAN-SPAM. Consider the following:
   - Organization chart to determine who is responsible for the financial institution's compliance with CAN-SPAM;
   - Process flow charts to determine how the financial institution's CAN-SPAM compliance is planned for, evaluated, and achieved;
   - Policies and procedures;
   - Marketing plans that reflect electronic communication strategies; and
   - Internal checklists, worksheets, and other relevant documents.
4. Review applicable audit and compliance review material, including work papers, checklists, and reports, to determine whether:
   - Procedures address CAN-SPAM provisions applicable to the institution;
   - Effective corrective action occurred in response to previously identified deficiencies;
   - Audits and reviews performed were reasonable and accurate;
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors; and
   - Frequency of the compliance review is satisfactory.
5. Review a sample of complaints to determine whether or not any potential violations of CAN-SPAM exist.
6. Based on the review of complaints that pertain to aspects of CAN-SPAM, revise the scope of examination focusing on the areas of particular risk. The verification procedures to be employed depend upon the adequacy of the institution's compliance program and level of risk identified.

Verification Procedures

1. Obtain a list of products or services that the financial institution has promoted with e- mail.
2. Obtain a sample of the e-mail messages to determine whether those messages had "commercial" promotion as their primary purpose.
3. Through review of e-mail messages whose primary purpose is "commercial," verify that the messages comply with the CAN-SPAM provisions:
   a. Do not use false or misleading transmission information [§7704(a)(1)] such as:
      - False or misleading header information;
      - A "from" line that does not accurately identify any person who initiated the message; and
      - Inaccurate or misleading identification of a protected computer used to initiate the message.
   b. Do not use deceptive subject headings. [§7704(a)(2)]
   c. Provide a functioning e-mail return address or other Internet-based response mechanism. [§7704(a)(3)]
   d. Provide a clear and conspicuous identification that the message is an advertisement or solicitation; clear and conspicuous notice of the opportunity to decline to receive further commercial e-mail messages from the sender; and a valid physical postal address of the sender. [§7704(a)(5)] Note: this provision does not apply to a commercial e-mail message if the recipient has given prior affirmative consent to receipt of the message.
   e. Do not reflect address harvesting, hijacking, or dictionary attacks. [Section 7704(b)(1, 2)]
   f. Provide a warning label (in the subject and within the message body) on commercial e-mail messages containing sexually oriented material. [Section 7704(d)]
4. Review any customer requests to opt out of receiving any additional e-mail messages from the institution. [Section 7704(a)(4)] Confirm that there are controls in place to discontinue commercial e-mail messages within 10 days of receipt of opt-out notification.

Conclusions

1. Summarize all findings, supervisory concerns, and regulatory violations.

2. For the violation(s), determine the root cause by identifying weaknesses in internal controls, audit and compliance reviews, training, management oversight, or other factors; also, determine whether the violation(s) are repetitive or systemic.
3. Identify action needed to correct violations and weaknesses in the institution's compliance program.
4. Discuss findings with the institution's management and obtain a commitment for corrective action.
5. Record violations according to agency policy to facilitate analysis and reporting.

References

Federal Trade Commission Resources

Consumer Website on SPAM Issues can be found at the FTC website.

Controlling the Assault of Non-Solicited Pornography and marketing Act of 2003

Job Aids

CAN-SPAM Examination Worksheet

This worksheet can be used to review audit work papers, to evaluate bank policies, to perform transaction testing, and to train as appropriate. Complete only those aspects of the worksheet that specifically relate to the issue being reviewed, evaluated, or tested, and retain those completed sections in the work papers

.

Examination Worksheet—CAN-SPAM	Yes	No
1. Does the financial institution initiate e-mail messages where the primary purpose is "commercial?" If No, stop here. If Yes, continue to question #2.		
For the questions below, every "No" answer indicates a potential violation of the regulation and/or an internal control deficiency that must be explained fully in the work papers.		
Prohibition Against Misleading Information		
2. In the sending of commercial e-mail messages, does the financial institution prohibit the following: [15 USC 7704(a)(1)]		
• Use of false or misleading header information in commercial e-mail messages.		
• Use of a "from" line that does not accurately identify the sender.		
• Inaccurate or misleading identification of a protected computer to send commercial e-mail messages in order to disguise the e-mail message's origin.		
3. Does the financial institution prohibit the use of deceptive or misleading headings in the subject line of commercial e-mail messages? [15 USC 7704(a)(2)]		
4. Does the financial institution use a functioning e-mail return address or other response mechanism to which consumers can reply or opt-out of receiving future commercial e-mail messages? [15 USC 7704(a)(3)]		
• Are these mechanisms displayed in a clear and conspicuous manner?		
Opt-Out Provisions		
5. Does the financial institution prohibit future transmissions of commercial e-mail messages within 10 business days of receiving the opt-out request? [15 USC 7704(a)(4)]		
Clear and Conspicuous Identification		
6. Does the financial institution's commercial e-mail message provide the following information clearly and conspicuously: [15 USC 7704(a)(5)]:		
• Identification that the e-mail message is an advertisement or solicitation. *NOTE: This provision does not apply to a commercial e-mail message if the recipient has given prior affirmative consent to receipt of the message.*		
• A notice of the option to decline further commercial e-mail messages from the sender.		
• A valid physical postal address of the sender.		
Transmission of Commercial E-mail Messages		
7. Does the financial institution prohibit the use of address harvesting or dictionary attacks as a means of obtaining consumer e-mail addresses? [15 USC 7704(b)(1)]		
8. Does the financial institution prohibit the automated creation of multiple e-mail accounts or online accounts that falsify e-mail message identification and transmit unlawful commercial e-mail messages? [15 USC 7704(b)(2)]		
9. Does the financial institution prevent the transmission of unlawful commercial e-mail messages by persons who access financial institution computers or computer network systems without authorization? [15 USC 7704(b)(3)]		

Examination Worksheet—CAN-SPAM	Yes	No
Sexually Oriented Material		
10. Does the financial institution refrain from transmitting sexually oriented material in commercial e-mail messages without warning labels in the subject line and message body? [15 USC 7704(d)]		