

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)]