

VIII. Privacy – CAN-SPAM

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

<http://www.ftc.gov/bcp/online/edcams/spam/index.html>

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

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

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.		
<i>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.</i>		
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. <i>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.</i>		
• 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)]		

VIII. Privacy – CAN-SPAM

Examination Worksheet—CAN-SPAM (continued)	Yes	No
Transmission of Commercial E-mail Messages (continued)		
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)]		
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)]		