Federal Deposit Insurance Corporation
550 17th Street NW, Washington, DC 20429

SECURITY STANDARDS FOR CUSTOMER INFORMATION

FIL-43-2000
July 6, 2000

TO: CHIEF EXECUTIVE OFFICER

SUBJECT: *Proposed Security Standards for Customer Information*

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision are jointly proposing the attached guidelines establishing standards for safeguarding customer information as required by the Gramm-Leach-Bliley Act (GLBA). The agencies are also seeking comment on the rescission of Year 2000 standards for safety and soundness. Comments are due by August 25, 2000.

The National Credit Union Administration has proposed essentially the same guidelines as part of its security program requirements.

GLBA requires the banking agencies to establish appropriate standards for financial institutions relating to the administrative, technical and physical safeguards of customer records and information. The standards' objectives are to:

- ensure the security and confidentiality of customer information;
- protect against any anticipated threats or hazards to the security or integrity of such information; and
- protect against unauthorized access to or use of customer information that could either result in substantial harm or inconvenience to any customer, or present a safety and soundness risk to the institution.

Information Security Program

The proposed guidelines describe the agencies' expectations for creating, implementing and maintaining an information security program. This program must include administrative, technical and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities.

The proposal describes the oversight role of the institution's board of directors in this process as well as management's continuing duty to evaluate and report to the board on the program's overall status. Institutions will be required to:

- identify and assess the risks that may threaten customer information;
- develop a written plan containing policies and procedures to manage and control these risks;

- implement and test the plan; and

- adjust the plan on a continuing basis to account for changes in technology, sensitivity of customer information, and internal or external threats to information security.

Risk Assessment

The guidelines describe the elements of a comprehensive risk-management plan designed to control identified risks and achieve the overall objective of ensuring the security and confidentiality of customer information. They identify the factors an institution should consider in evaluating the adequacy of its policies and procedures to effectively manage these risks commensurate with the sensitivity of the information, as well as the complexity and scope of the institution and its activities. The agencies intend that these elements accommodate institutions of varying sizes, scopes of operation and risk-management structures.

The agencies invite comment on the degree of detail that should be included in the guidelines regarding the risk-management program, which elements should be specified in the guidelines, and any other components of a risk-management program that should be included.

Involvement of the Board of Directors and Management

The guidelines describe the responsibilities of the board of directors and management in developing and implementing an information security program. The board's responsibilities are to:

- approve the institution's written information security policy and program that comply with these guidelines; and

- oversee efforts to develop, implement and maintain an effective information security program, including regularly reviewing reports filed by management.

Management's three responsibilities in developing an information security program are to:

- evaluate how changing business arrangements (e.g., mergers and acquisitions, alliances and joint ventures, and outsourcing arrangements) and changes to customer information systems impact the institution's security program;

- document compliance with guidelines; and

- keep the board informed of the current status of the institution's information security program, i.e., report to the board regularly on the overall status of the information security program, including material matters related to:

    - risk assessment;

    - risk-management and control decisions;

    - testing results;

- attempted or actual security breaches or violations and responsive actions taken by management; and

- any recommendations for improvements to the information security program.

The agencies specifically invite comment on the appropriate frequency of reports to the board, as well the designation of a Corporate Information Security Officer or other individual responsible for developing and administering the institution's information security program.

Outsourcing Arrangements

An institution should exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect customer information and customer information systems consistent with these guidelines. The agencies welcome comments on the appropriate treatment of outsourcing arrangements.

Community Banks

The agencies invite comment on how this proposal would impact community banks. The agencies recognize that community banks operate with more limited resources than larger institutions and may present a different risk profile. Therefore, the agencies specifically request comment on the impact of this proposal on community banks' current resources and available personnel with the requisite expertise. Comments should address whether the standards are reasonable and realistic for community banks, and whether the proposed regulation's goals could be achieved for community banks through an alternative approach.

For more information, please contact Jeffrey M. Kopchik (202-898-3872) or Thomas J. Tuzinski (202-898-6748) in the FDIC's Division of Supervision, or Robert A. Patrick (202-898-3757) in the FDIC's Legal Division.

James L. Sexton
Director

Attachment: June 26, 2000 Federal Register, pages 39471-39489
HTML or PDF (77 KB File - PDF Help or Hard Copy)

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (800-276-6003 or (703) 562-2200).