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

SECURITY STANDARDS FOR CUSTOMER INFORMATION

FIL-22-2001
March 14, 2001

TO: CHIEF EXECUTIVE OFFICER AND COMPLIANCE OFFICER

SUBJECT: *Guidelines Establishing Standards for Safeguarding 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 have jointly approved and issued the attached guidelines establishing standards for safeguarding customer information as required by the Gramm-Leach-Bliley Act (GLBA).

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 result in substantial harm or inconvenience to any customer.

Information Security Program

The 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 guidelines also describe the oversight role of the institution's board of directors in this process and its continuing duty to evaluate and oversee the program's overall status. Institutions are 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 will provide general parameters for institutions of varying sizes, scopes of operation and risk-management structures.

Involvement of the Board of Directors

The guidelines describe the responsibilities of the board of directors and management in developing and implementing an information security program. The board, or an appropriate board committee, is expected to:

- approve the institution's written information security program that complies with these guidelines; and
- oversee efforts to develop, implement and maintain an effective information security program, including regularly reviewing reports filed by management.

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, an institution should exercise appropriate due diligence in managing and monitoring its outsourcing arrangements.

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.

Michael J. Zamorski
Acting Director

Attachment: Feb. 1, 2001, *Federal Register*, pages 8616-8641
HTML or PDF (126 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).