
Joint Release

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency
Office of Thrift Supervision**

For immediate release

January 17, 2001

Agencies Adopt Guidelines for Customer Information Security

The federal bank and thrift regulatory agencies have sent to the Federal Register joint guidelines for safeguarding confidential customer information. The guidelines implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA), and will be effective on July 1, 2001.

The GLBA requires the agencies to establish standards for financial institutions relating to administrative, technical and physical safeguards for customer records and information. These safeguards are to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of these records, and protect against unauthorized access to or use of these records or information that would result in substantial harm or inconvenience to a customer.

The guidelines require financial institutions to establish an information security program to: (1) identify and assess the risks that may threaten customer information; (2) develop a written plan containing policies and procedures to manage and control these risks; (3) implement and test the plan; and (4) adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security. Each institution may implement a security program appropriate to its size and complexity and the nature and scope of its operations.

The guidelines outline specific security measures that institutions should consider in implementing a security program. A financial institution must adopt those security measures determined to be appropriate.

The guidelines also outline responsibilities of directors of financial institutions in overseeing the protection of customer information. The board of directors should oversee an institution's efforts to develop, implement, and maintain an effective information security program and approve written information security policies and programs.

The guidelines require financial institutions to oversee their service provider arrangements in order to protect the security of customer information maintained or processed by service providers. Each institution must exercise due diligence in selecting its service providers, and require its service providers by contract to implement security measures that safeguard customer information. Where indicated by an institution's risk assessment, the institution must also monitor its service providers by reviewing audits, summaries of test results, or other equivalent evaluation of its service providers, to confirm that they have satisfied their contractual obligations.

#

Federal Reserve:	David Skidmore	(202) 452-2955
FDIC:	David Barr	(202) 898-699
OCC:	Bob Garsson	(202) 874-5770
OTS:	Paul Lockwood	(202) 906-6913

Attachment: 501 Final Rule

[PDF](#) (180 KB File - [PDF Help](#) or [Hard Copy](#))

FDIC-PR-4-2001