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 June 21, 2000

AGENCIES PROPOSE STANDARDS FOR CUSTOMER INFORMATION SECURITY

The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision jointly requested comment today on a proposed rule establishing standards for safeguarding confidential customer information. The proposed rule would implement section 501 (b) of the Gramm-Leach-Bliley Act (GLBA).

Comments will be accepted until August 25, 2000.

The law requires the agencies to establish standards for financial institutions relating to administrative, technical and physical safeguards for customer records and information. These safeguards are intended 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 proposed rule would provide that financial institutions establish an information security program that would require them 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.

The proposed rule outlines specific factors that banks should consider in implementing a security program. Among other factors, banks should evaluate their controls on access to customer information and their policies for encrypting customer information while it is being transmitted or stored on networks to which unauthorized persons may have access.

Financial institutions should test, on a regular basis, key controls, systems and procedures to confirm that they meet the objectives of their security programs. The proposed guidelines suggest that tests should be conducted by independent third parties or by staff independent of those that develop or maintain the security program.

The agencies seek comment on the need for specific types of tests, such as penetration or intrusion detection tests.

The proposed rule also outlines responsibilities of directors and management of financial institutions in overseeing the protection of customer information. An institution's board of directors should approve written information security policies and programs, and oversee management's efforts to develop, implement and maintain an effective information security program. Management should evaluate the impact of changing business arrangements, such as mergers and joint ventures, document compliance with the security standards, and report to the board on the overall status of the program.

The agencies seek comments on various aspects of the proposal, including its impact on community banks that operate with more limited resources and which may have a different risk profile than larger banks. Comments are also sought on whether the final standards should be guidelines or regulations.

# # #

Media Contacts:
Federal Reserve: David Skidmore (202) 452-2955
FDIC: David Barr (202) 898-6992
OCC: Bob Garsson (202) 874-5770
OTS: Bill Fulwider (202) 906-6913
FDIC-PR-44-2000