OCC 2001-8

# OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

| | | | |
|---|---|---|---|
| Subject: | Guidelines Establishing Standards for Safeguarding Customer Information | Description: | Final Guidelines |

**TO:** Chief Executive Officers and Compliance Officers of All National Banks, Federal Branches and Agencies, Service Providers and Software Vendors, Department and Division Heads, and All Examining Personnel

## PURPOSE

The purpose of this bulletin is to alert you to the joint-agency issuance of the attached final "Guidelines Establishing Standards for Safeguarding Customer Information" and to highlight provisions of these guidelines. The guidelines are mandated by Section 501 of the Gramm–Leach–Bliley Act of 1999 (GLBA), and are effective July 1, 2001. The guidelines affect all national banks, federal branches and federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisors).[1] The guidelines describe the Office of the Comptroller of the Currency's (OCC's) expectations for the creation, implementation, and maintenance of a comprehensive information security program.

## BACKGROUND

Section 501 of the GLBA requires the OCC and other federal banking agencies to establish appropriate standards for the administrative, technical, and physical safeguards for customers' "nonpublic personal information." The OCC has done so by issuing guidelines that require each national bank to establish an information security program.

A bank's information security program must be designed 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 such information that would result in substantial harm or inconvenience to any customer.

Because the guidelines codify existing agency guidance, banks should already have existing information security programs that identify and control risks to information and information systems. While the guidelines cover only "customer information" as that term is defined, the

[1] Certain functionally regulated subsidiaries, such as brokers, dealers, and investment advisors will be subject to security regulations issued by the Securities and Exchange Commission. Insurance entities may be subject to security regulations issued by their respective state insurance authorities.

OCC encourages banks to use the approach provided by the Guidelines to protect all customer and bank records.

**Highlights of the Guidelines**

The guidelines allow each institution the discretion to design an information security program that suits its particular size and complexity and the nature and scope of its activities. The guidelines take a process-based approach that is consistent with OCC guidance, notably OCC Bulletin 98-3 ("Technology Risk Management"), issued February 4, 1998; and OCC Bulletin 2000-14 ("Infrastructure Threats -- Intrusion Risks"), issued May 15, 2000.

*Role of the Board of Directors.* The board of directors or an appropriate committee of the board is responsible for approving the bank's written information security program and overseeing the program's development, implementation, and maintenance, including assigning responsibility for its implementation. At least once a year, bank management should report to the board or an appropriate committee of the board on the overall status of the information security program and the bank's compliance with the guidelines.

*Identify and Assess Risk.* The bank should first assess risks to its customer information. A bank's risk assessment should identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. Additionally, the risk assessment should consider the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information. Finally, the assessment should consider the sufficiency of existing policies, procedures, customer information systems, and other arrangements intended to control the risks identified.

*Manage and Control of Risk.* The bank should design an information security program to control the identified risks, commensurate with the sensitivity of the information and the complexity and scope of the bank's activities. The guidelines highlight eight security measures that banks should consider and adopt if appropriate.

The information security program also should include training for bank staff and regular testing of the key controls, systems, and procedures. The nature and frequency of the tests should be determined by the bank's risk assessment. To ensure objectivity, tests should be conducted or reviewed by third parties or staff who are independent of those who develop or maintain the security programs.

*Oversee Service Provider Arrangements.* Banks also have an obligation to oversee their service providers. Banks that use service providers should exercise appropriate due diligence in selecting them, including conducting a review of the measures taken by the service providers to protect customer information. The contract between the bank and the service provider must require the provider to implement appropriate measures designed to meet the objectives of the guidelines. Wherever indicated by a bank's risk assessment, the bank should monitor its service providers to confirm they are implementing the agreed-upon security measures. As part of this

monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

*Adjust the Program.* Risks to customer information change over time with changes in technology, the sensitivity of customer information, internal or external threats to information, and the bank's own business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems. Therefore, banks should monitor, evaluate, and adjust, as appropriate, their information security program. The OCC expects banks to make the appropriate changes to their information security programs before any bank-initiated changes are made to their customer information systems, such as changes to accommodate new services.

*Implement the Guidelines.* The guidelines are effective on July 1, 2001. However, there is a two-year grandfathering provision for service provider contracts. Existing service provider contracts (namely, contracts entered into until March 5, 2001) do not have to be renegotiated to comply with the Guidelines until July 1, 2003.

**RESPONSIBLE OFFICE**

Questions regarding this banking issuance should be directed to John Carlson, senior advisor for Bank Technology, (202) 874-5013; Aida Plaza Carter, director for Bank Information Technology Operations, (202) 874-4740; or Deborah Katz, senior attorney, Legislative and Regulatory Activities Division, (202) 874-5090.

_____

Clifford A. Wilke
Director, Bank Technology Division

Attachment--66 FR 8616