



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM

WASHINGTON, D. C. 20551

DIVISION OF BANKING
SUPERVISION AND REGULATION

DIVISION OF CONSUMER
AND COMMUNITY AFFAIRS

SR 05-23 / CA 05-10
December 1, 2005

**TO THE OFFICER IN CHARGE OF SUPERVISION AND
APPROPRIATE SUPERVISORY AND EXAMINATION
STAFF AT EACH FEDERAL RESERVE BANK, AND TO
BANKING ORGANIZATIONS SUPERVISED BY THE
FEDERAL RESERVE**

**SUBJECT: Interagency Guidance on Response Programs for Unauthorized Access to
Customer Information and Customer Notice**

This joint Supervision and Regulation and Consumer Affairs Letter establishes the Federal Reserve's expectations for financial institutions and supervisory personnel with respect to the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (Guidance), which became effective upon publication in the *Federal Register* on March 29, 2005.¹

The Guidance interprets the *Interagency Guidelines Establishing Information Security Standards* (Security Guidelines)² and states that each financial institution should implement a response program to address unauthorized access to customer information maintained by the institution or its service providers.³ The Guidance describes the components of a response program, including procedures to notify customers about incidents that involve unauthorized access to *sensitive* customer information.

Sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

The Guidance provides that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.

Notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for a delay.

The Guidance also provides that a financial institution should notify its primary federal regulator of a security breach involving sensitive customer information, whether or not the institution notifies its customers. A financial institution experiencing such a breach should promptly notify its supervisory central point of contact at its Reserve Bank and provide information on the nature of the incident and on whether law enforcement authorities were notified or a Suspicious Activity Report (SAR) was or will be filed. When reporting security breaches involving sensitive customer information, an institution should provide the central point of contact with information on the steps taken to contain and control the incident, the number of customers potentially affected, whether customer notification is warranted, and whether a service provider was involved. A financial institution should not delay providing prompt initial notification to its central point of contact.

When evaluating the adequacy of a financial institution's information security program required by the Security Guidelines, the Federal Reserve will consider whether the bank has developed and implemented a response program including notification procedures as described in the Guidance. An institution's response program should contain procedures for the following:

1. Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;
2. Notifying the institution's primary federal regulator as soon as possible once the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
3. Complying with applicable suspicious activity reporting regulations and guidance to ensure appropriate law enforcement authorities are notified in a timely manner;
4. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts; and
5. Notifying customers as soon as possible when it is determined that misuse of sensitive customer information has occurred or is reasonably possible.

The Guidance states that a financial institution's contract with each service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program. While the Guidance states that it is the responsibility of the financial institution to notify the institution's primary regulator, an institution may authorize or contract with its service provider to notify the institution's regulator of a security incident on its behalf.

When evaluating the adequacy of a financial institution's information security program or a specific security breach incident, the Federal Reserve will take into account the good faith efforts made by each financial institution to develop a response program that is consistent with the Guidance, together with all other relevant circumstances. The Federal Reserve may treat a financial institution's failure to implement the Guidance as an unsafe and unsound practice.

Upon receipt of notification of a security breach, unauthorized access, or misuse of sensitive customer information, Reserve Banks should notify appropriate Board staff if it has been determined that misuse of the information has occurred or is reasonably possible and customer notification will likely be required. Board staff will follow the progress of the incident and will utilize this information to inform future supervisory guidance and identify trends in information security developments.

This supervisory letter should be distributed to the appropriate management personnel at financial institutions supervised by the Federal Reserve. If you have any questions concerning this Guidance, please contact Stacy Coleman, Assistant Director, Operational and IT Risk Section, at (202) 452-2934, Suzanne Killian, Assistant Director for Reserve Bank Oversight, at (202) 452-2090, or John Gibbons, Supervisory Financial Analyst, at (202) 452-6409.

Richard Spillenkothen
Director
Division of Banking
Supervision and Regulation

Sandra Braunstein
Director
Division of Consumer
and Community Affairs

Attachment:

[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#) (413 KB PDF)

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

Notes:

1. The Security Guidelines apply to customer information maintained by or on behalf of bank holding companies and state member banks (banks), and their nonbank subsidiaries or affiliates, except for brokers, dealers, persons providing insurance, investment companies, and investment advisors, for which the Board has supervisory authority. The Security Guidelines also apply to customer information maintained by or on behalf of Edge corporations, agreement corporations, and uninsured state-licensed branches or agencies of a foreign bank. [Return to text](#)
2. 12 CFR part 208, app. D-2 and 12 CFR part 225, app. F. [Return to text](#)
3. Under the Security Guidelines, customer information means any record, whether in paper, electronic, or other form, containing nonpublic personal information about an individual who has obtained a financial product or service from the institution that is to be used primarily for personal, family, or household purposes and who has an ongoing relationship with the institution. [Return to text](#)

