Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-27-2005
April 1, 2005

FINAL GUIDANCE ON RESPONSE PROGRAMS

Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Summary: The FFIEC agencies are jointly issuing the attached interpretive guidance for financial institutions to develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Officer
Compliance Officer
Legal Counsel

Related Topics:
Interagency Guidelines Establishing Information Security Standards

FFIEC Information Security Handbook issued January 2003

Attachment:
Federal Register notice

Contact:
Senior Policy Analyst, Jeffrey M. Kopchik, JKopchik@fdic.gov, (202) 898-3872
Examination Specialist, Kathryn M. Weatherby, Kweatherby@fdic.gov, (202) 898-6793
Counsel, Legal Division, Robert A. Patrick RPatrick@fdic.gov, (202) 898-3757

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2005/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

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 (1-877-275-3342 or 202-416-6940).

Highlights:

- The guidance is an interpretation of section 501(b) of the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines Establishing Information Security Standards (12 CFR 364, Appendix B).
- The interpretive guidance states that financial institutions should develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider.
- The interpretive guidance describes the appropriate elements of a financial institution's response program, including customer notification procedures.
- The guidance is effective immediately. Financial institutions should implement the guidance as soon as possible.

FINAL GUIDANCE ON RESPONSE PROGRAMS
Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

The Federal Financial Institutions Examination Council (FFIEC) agencies are issuing the attached interpretive guidance stating that every financial institution should develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider.

The agencies are issuing the interpretive guidance under the authority of section 501(b)(3) of the Gramm-Leach-Bliley Act (GLBA), which states the information security standards established by the agencies must include various safeguards to protect against not only "unauthorized access to" but also the "use of" customer information in a manner that could result in "substantial harm or inconvenience to any customer."

Components of a Response Program

At a minimum, an institution's response program should contain procedures for:

- Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;
- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Consistent with the agencies' Suspicious Activity Report (SAR) regulations, filing a timely SAR, and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities;
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and
- Notifying customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it.

When an incident of unauthorized access to sensitive customer information involves customer information systems maintained by an institution's service provider, it is the financial institution's responsibility to notify its customers and regulator. However, an

institution may authorize or contract with its service provider to notify the institution's customers or regulator on its behalf.

Sensitive Customer Information

For purposes of this guidance, 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. It also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as user name and password or password and account number.

When Customer Notice Should be Provided

The interpretive guidance states that a financial institution should provide a notice to its customers whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

Customer Notice

Customer notice should be given in a clear and conspicuous manner. The notice should include the following items:

- Description of the incident;
- Type of information subject to unauthorized access;
- Measures taken by the institution to protect customers from further unauthorized access;
- Telephone number customers can call for information and assistance; and
- Remind customers to remain vigilant over next twelve to twenty four months, and report suspected identity theft incidents to the institution.

The guidance encourages financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

Delivery of Customer Notice

Customer notice should be delivered in a manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Effective Date

The guidance is an interpretation of existing provisions in section 501(b) of the GLBA and Information Security Guidelines. Therefore, a delayed effective date is not required. Financial institutions should implement the interpretive guidance as soon as possible. The agencies recognize that not every financial institution currently has a response program that is consistent with the interpretive guidance. The agencies will take into account the good faith efforts made by each institution to develop a response program that is consistent with the interpretive guidance, however; any financial institution experiencing a breach in security that includes unauthorized access to customer information is expected to respond promptly in a manner consistent with the guidance, and provide customer notice, if warranted.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection