SUPPORTING STATEMENT
Notice Regarding Unauthorized Access to Customer Information
(3064-0145)

INTRODUCTION

The FDIC requests OMB approval for the collection of information captioned above. The collection is scheduled to expire on September 30, 2009.

This collection is contained in *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (published jointly by the FDIC, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision at 70 FR 15736, attached). The *Guidance* describes the Agencies' expectations regarding a response program, including customer notification procedures, that a financial institution should develop and apply under the circumstances described in the Appendix to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The *Guidance* advises financial institutions when and how they might: (1) develop notices to customers; (2) in certain circumstances defined in the *Guidance*, determine which customers should receive the notices and send the notices to customers.

A. JUSTIFICATION

1. Circumstances and Need

The guidance interprets interagency customer information security guidelines that require financial institutions to implement information security programs designed to protect their customers' information. The interpretation describes the components of a response program and sets a standard for providing notice to customers affected by unauthorized access to or use of customer information that could result in substantial harm or inconvenience to those customers, thereby reducing the risk of losses due to fraud or identity theft.

The guidance states that "an institution should notify affected customers when it becomes aware of unauthorized access to sensitive customer information unless the institution, after an appropriate investigation, reasonably concludes that misuse is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers, including monitoring affected customers' accounts for unusual or suspicious activity." Developing and providing the notices, a third party disclosure, is considered a collection of information under the Paperwork Reduction Act.

2. Use of the Information Collected

The collection is intended to help financial institutions develop administrative, technical, and physical safeguards to: (1) insure the security and confidentiality of customer records

and information; (2) protect against anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

A response program, of which this collection is a critical part, contains policies and procedures that enable the financial institution to: (a) assess the situation to determine the nature and scope of the incident, and identify the information systems and types of customer information affected; (b) notify the institution's primary Federal regulator and, in accordance with applicable regulations and guidance, file a Suspicious Activity Report and notify appropriate law enforcement agencies; (c) take measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls; and (d) address and mitigate harm to individual customers.

3. Use of Technology to Reduce Burden

Respondents may use any technology they wish to reduce the burden associated with this collection.

4. Effort to Identify Duplication

There is no duplication.

5. Minimizing the Burden on Small Entities

The collection applies to all institutions, regardless of size.

6. Consequences of Less Frequent Collections

The FDIC believes that less frequent collection (a less stringent disclosure standard) would result in unacceptable harm to customers of financial institutions.

7. Special Circumstances

No special circumstances exist.

8. Consultation with Persons Outside the FDIC

Extensive interagency collaboration was involved in creating this collection. Further, when the *Guidance* was first developed in 2003, it was published in proposed form and revised based on comments received.

9. Payment or Gift to Respondents

Not applicable.

10. Confidentiality

Financial institutions would treat these disclosure requirements with the same degree of confidentiality as other disclosures of sensitive customer information.

11. Information of a Sensitive Nature

The disclosure of this information would be limited to account holders.

12. Estimate of Annual Burden

It is estimated that it will take covered institutions 29 hours per incident (three business days) to determine which customers should receive the notice and notify the customers. Bank supervisory experience indicates that just under two percent of covered institutions [5,044] annually will experience an incident of unauthorized access to customer information resulting in customer notification. Thus, the burden associated for this collection of information may be summarized as follows:

Number of FDIC regulated banks that will notify customers: 100

Estimated Time per response: 29 hours

Total Estimated Annual Burden: $2, 900 hours

Estimate of annualized cost: 2,900 hours x $50/hour = $145,000.

13. Total Annual Cost Burden

Not applicable.

14. Annualized Cost to the Federal Government

Negligible.

15. Reason for Program Changes or Adjustments

It is estimated that all covered institutions have developed and produced the notices described in the Guidance. The estimated burden herein is thus based upon bank supervisory experience that approximately two percent of covered institutions [5044 x .02 =100] annually will experience an incident of unauthorized access to customer information resulting in customer notification.

16. Publication

Not applicable.

17. Display of Expiration Date

Not applicable.

18. Exceptions to Certification

None.

B. Statistical Methods

Not applicable.

Attachments

1. Underlying statutory authority (section 501(b) of the Gramm-Leach-Bliley Act).
2. *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (70 FR 15736).
3. First *Federal Register* notice (74 FR 32609; Second *Federal Register* notice