Supporting Statement for
OMB Control No. 1557-0227
Guidance Regarding Unauthorized Access
to Customer Information

INTRODUCTION

The OCC requests that OMB extend its approval for the collections of information contained in 12 CFR Part 30, Appendix B, Supplement A, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*. 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 information collections in the Guidance require financial institutions to: (1) develop notices to customers and (2) in certain circumstances defined in the Guidance, determine which customers should receive the notices and send the notices to customers.

JUSTIFICATION

1. Circumstances that make the collection necessary

This collection is a notice requirement contained in guidance that requires financial institutions to develop programs to respond to incidents of unauthorized access to customer information, including procedures for notifying customers under certain circumstances. The guidance was adopted jointly by the OCC, the Board of Governors of the Federal Reserve System, the FDIC, and the OTS.

The guidance interprets the interagency customer information security guidelines (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." This third party disclosure is considered a collection of information under the Paperwork Reduction Act.

2. Use of the Information Collected

Section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6901) requires the OCC to establish standards for national banks relating to administrative, technical, and physical safeguards to: (1) insure the security and confidentiality of customer records and information; (2) protect against any 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.

The Security Guidelines implementing section 501(b) require each bank to consider and adopt a response program, if appropriate, that specifies actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information.

The notice covered by this collection must be a part of a national bank's response program. The response program should contain policies and procedures that enable the financial institution to: (1) assess the situation to determine the nature and scope of the incident, and identify the information systems and types of customer information affected; (2) 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; (3) 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 (4) address and mitigate harm to individual customers.

3. Consideration of the use of improved information technology

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

4. Efforts to identify duplication

There is no duplication.

5. Methods used to minimize burden if the collection has a significant impact on a substantial number of small entities

The collection applies to all national banks, regardless of size. Further, this information collection does not have a significant impact on a substantial number of small entities.

6. Consequences to the Federal program if the collection were conducted less frequently

The OCC believes that less frequent collection (a less stringent disclosure standard) would result in unacceptable harm to customers of national banks. However, the agencies are seeking comment on the appropriateness of the disclosure standard.

7. Special circumstances necessitating collection inconsistent with 5 CFR part 1320

No special circumstances exist.

8. Consultation with persons outside the agency

The collection was published for public comment at 75 FR 5641 (February 3, 2010). No comments were received.

9. Payment to respondents

Not applicable.

10. Confidentiality

National banks 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 customers.

12. Burden estimate

The burden associated with this collection of information is summarized as follows:

Number of Respondents: 25.

Estimated Time per Respondent:

Developing notices: 16 hrs. x 25 respondents = 400 hours

Notifying customers: 20 hrs. x 25 respondents = 500 hours

Estimated average burden per respondent: 36 hours.

Total Estimated Annual Burden: 900 hours

13. Estimate of annualized costs to respondents

Not applicable.

14. Estimate of annualized costs to the government

Not applicable.

15. Changes to burden

The change in burden is due to the availability of data reflecting the number of national banks that notified customers of unauthorized access and the number of times customers were notified. Our prior submission used the total number of national banks for the number of respondents because this data was not available. In addition, the data provided more accurate information on the time taken to respond.

Prior burden:

Estimated number of Respondents: 2,200.
Estimated Average Burden per Respondent: 24.4746 hours.
Total Estimated Annual Burden: 53,844 hours.

Current Burden:

Estimated Number of Respondents: 25.
Estimated Average Burden per Respondent: 36 hours.
Total Estimated Annual Burden: 900 hours.

Difference:

Estimated Number of Respondents: - 2,175.
Estimated Average Burden per Respondent: + 11.5254 hours.
Total Estimated Annual Burden: - 52,944 hours.

16. Information regarding collections whose results are planned to be published for statistical use

The results of these collections will not be published for statistical use.

17. Display of expiration date

Not applicable.

18. Exceptions to certification statement

None.

A. STATISTICAL METHODS

Not applicable.