

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

**A. Justification**

**1. *Circumstances that Make the collection necessary:***

Section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801) requires the OCC to establish appropriate standards for national banks relating to administrative, technical, and physical safeguards:

(1) To insure the security and confidentiality of customer records and information;

(2) To protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) To protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer.

The Interagency Guidelines Establishing Information Security Standards, 12 CFR Part 30, Appendix B and Part 170, Appendix B (collectively, Security Guidelines), which implement section 501(b), require each entity supervised by the OCC (supervised institution) to consider and adopt a response program, if appropriate, that specifies actions to be taken when the supervised institution suspects or detects that unauthorized individuals have gained access to customer information.

**2. *Use of the information:***

The Interagency Guidance on Response Programs for Unauthorized Customer Information and Customer Notice (Breach Notice Guidance<sup>1</sup>), which provides interpretation of the Security Guidelines, states that, at a minimum, a supervised 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 its primary Federal regulator as soon as possible when the supervised institution becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information;

---

<sup>1</sup> 12 CFR Part 30, Appendix B, Supplement A.

(3) Consistent with the OCC's Suspicious Activity Report regulations, notifying appropriate law enforcement authorities, as well as filing a timely SAR in situations in which a Federal criminal violation requires immediate attention, such as when a reportable violation is ongoing;

(4) Taking appropriate steps to contain and control the incident in an effort to prevent further unauthorized access to, or use of, customer information (for example, by monitoring, freezing, or closing affected accounts), while preserving records and other evidence; and

(5) Notifying customers when warranted.

This collection of information covers the notice provisions in the Breach Notice Guidance.

**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:***

Not applicable.

**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.

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

No special circumstances exist.

**8. *Efforts to consult with persons outside the agency:***

The collection was published for public comment at 81 FR 21666 (April 12, 2016). No comments were received.

**9. Payment or gift to respondents:**

Not applicable.

**10. Any assurance of confidentiality:**

The information collected is kept confidential to the extent permissible by law.

**11. Justification for questions 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:

Estimated Number of Respondents: 20.

Developing notices: 16 hrs. x 20 respondents = 320 hours

Notifying customers: 20 hrs. x 20 respondents = 400 hours

Estimated average burden per respondent: 36 hours.

Total Estimated Annual Burden: 720 hours

**Cost of Hour Burden**

**720 x \$101 = \$72,720**

To estimate average hourly wages we reviewed data from May 2015 for wages (by industry and occupation) from the U.S. Bureau of Labor Statistics (BLS) for depository credit intermediation (NAICS 522100). To estimate compensation costs associated with the rule, we use \$101 per hour, which is based on the average of the 90th percentile for seven occupations adjusted for inflation (two percent), plus an additional 30 percent to cover private sector benefits. Thirty percent represents the average private sector costs of employee benefits.

**13. Estimate of total annual costs to respondents (excluding cost of hour burden in Item #12:**

Not applicable.

**14. Estimate of annualized costs to the Federal government:**

Not applicable.

**15. Change in burden:**

Current burden: 12,384 hours.  
Revised burden: 720 hours.  
Difference: - 11,664 hours.

The decrease in burden is due to the availability of more accurate burden estimates.

**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. Reasons for not displaying OMB approval expiration date:**

Not applicable.

**18. Exceptions to certification statement:**

None.

**B. Collections of Information Employing Statistical Methods.**

Not applicable.