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(b)) requires the OCC to establish appropriate standards for national banks, Federal savings associations, Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) 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 (Security Guidelines), which implement section 501(b), require each entity supervised by the OCC to consider and adopt a response program, as 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 Access to Customer Information and Customer Notice (Breach Notice Guidance),[1] which interprets the Security Guidelines, states that, at a minimum, a supervised institution's response program should contain procedures for:

(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;

(3) Notifying appropriate law enforcement authorities in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, consistent with the OCC's Suspicious Activity Report regulations;

[1] 12 CFR part 30, appendix B, supplement A.

(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.

The Breach Notice Guidance states 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 the misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.

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. If the collection of information impacts small businesses or other small entities, describe any methods used to minimize burden.

Appendix B to 12 CFR part 30 applies to all OCC-supervised institutions regardless of asset size. The OCC believes that all institutions should prepare customer response programs. However, the OCC recognizes that an institution's program will vary depending on the size and complexity of the institution and the nature and scope of its activities.

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 87 FR 20932, April 8, 2022. No comments were received.

9. Payment or gift to respondents:

Not applicable.

10. Any assurance of confidentiality:

The information collected is kept private 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 $119.63 = $86,133.60

To estimate wages the OCC reviewed May 2021 data for wages (by industry and occupation) from the U.S. Bureau of Labor Statistics (BLS) for credit intermediation and related activities (NAICS 5220A1). To estimate compensation costs associated with the rule, the OCC uses $119.63 per hour, which is based on the average of the 90th percentile for six occupations adjusted for inflation (6.1 percent as of Q1 2022), plus an additional 32.8 percent for benefits (based on the percent of total compensation allocated to benefits as of Q4 2021 for NAICS 522: credit intermediation and related activities).

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:

There is no change in burden.

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.