

disclose information pursuant to the proposed Guidance.

## OCC

*Number of Respondents:* 2,200.

*Estimated Time per Response:*

Developing notices: 20 hrs.  $\times$  2,200 = 44,000 hours.

Notifying customers: 24 hrs.  $\times$  44 = 1,056 hours.

*Total Estimated Annual Burden =* 45,056 hours.

## Board

*Number of Respondents:* 6,692.

*Estimated Time per Response:*

Developing notices: 20 hrs.  $\times$  6,692 = 133,840 hours.

Notifying customers: 24 hrs.  $\times$  134 = 3,216 hours.

*Total Estimated Annual Burden:* 137,056 hours.

## FDIC

*Number of Respondents:* 5,500.

*Estimated Time per Response:*

Developing notices: 20 hrs.  $\times$  5,500 = 110,000 hours.

Notifying customers: 24 hrs.  $\times$  110 = 2,640 hours.

*Total Estimated Annual Burden:* 112,640 hours.

## OTS

*Number of Respondents:* 961.

*Estimated Time per Response:*

Developing notices: 20 hrs.  $\times$  961 = 19,220 hours.

Notifying customers: 24 hrs.  $\times$  19 = 456 hours.

*Estimated Total Annual Burden:* 19,676 hours.

## Appendix—Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

### I. Background

This Guidance<sup>1</sup> interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Security Guidelines")<sup>2</sup> and describes the Agencies' expectations regarding the response programs, including customer notification procedures, that a financial institution should develop and apply to address unauthorized access to or use of customer information that could result

in substantial harm or inconvenience to a customer.

### Interagency Security Guidelines

Section 501(b) of the GLBA required the Agencies to establish appropriate standards for financial institutions subject to their jurisdiction that include administrative, technical, and physical safeguards, to protect the security and confidentiality of customer information.<sup>3</sup> Accordingly, the Agencies issued Security Guidelines requiring every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

### Risk Assessment and Controls

The Security Guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and
- The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.<sup>4</sup>

Following the assessment of these risks, the Security Guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines,<sup>5</sup> and adopt those that are appropriate for the institution, including:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Background checks for employees with responsibilities for access to customer information; and
- Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.<sup>6</sup>

<sup>3</sup> The term "customer information" is the same term used in the Security Guidelines and means any record containing nonpublic personal information whether in paper, electronic, or other form, maintained by or on behalf of the institution.

<sup>4</sup> See Security Guidelines Paragraph III.B.

<sup>5</sup> See Security Guidelines Paragraph III.C.

<sup>6</sup> See Security Guidelines Paragraph III.D.

### Service Providers

The Security Guidelines direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.<sup>7</sup> Consistent with existing guidance issued by the Agencies, an institution's contract with its service provider should require the service provider to fully disclose to the institution information relating to any breach in security resulting in an unauthorized intrusion into the institution's customer information systems maintained by the service provider.<sup>8</sup> In view of these contractual obligations, the service provider would be required to take appropriate actions to address incidents of unauthorized access to or use of the financial institution's customer information to enable the institution to expeditiously implement its response program.<sup>9</sup>

### Response Program

As internal and external threats to the security of customer information are reasonably foreseeable and may lead to the misuse of customer information, the Agencies expect every financial institution to develop a response program to protect against the risks associated with these threats. The response program should include measures to protect customer information in customer information systems maintained by the institution or its service providers. The Agencies expect that customer notification will be a component of an institution's response program, as described below.

## II. Components of a Response Program

A response program should be a key part of an institution's information security

<sup>7</sup> See Security Guidelines Paragraphs II.B. and III.D.

<sup>8</sup> See Federal Reserve SR Ltr. 00-04, Outsourcing of Information and Transaction Processing, Feb. 9, 2000; SR Ltr. 00-17, Guidance on Risk Management of Outsourced Technology Services, Nov. 30, 2000; OCC Bulletin 2001-47, "Third-party Relationships Risk Management Principles," Nov. 1, 2001; AL 2000-12, "FFIEC Guidance on Risk Management of Outsourced Technology Services," Nov. 28, 2000; FDIC FIL 81-2000, Risk Management of Technology Outsourcing, Nov. 29, 2000; FIL 68-99, Risk Assessment Tools and Practices for Information System Security, July 7, 1999; OTS Thrift Bulletin 82, Third Party Arrangements, Mar. 4, 2003; OTS CEO Memorandum 133, Risk Management of Technology Outsourcing, Dec. 13, 2000; CEO Memorandum 109, Transactional Web Sites, June 10, 1999; CEO Memorandum 70, Statement on On-Line Personal Computer Banking, June 23, 1997.

<sup>9</sup> The Agencies note that, in addition to contractual obligations to a financial institution, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the FTC. 12 CFR part 314 applies to the handling of all customer information possessed by any financial institution subject to the jurisdiction of the FTC, regardless of whether such information pertains to individuals with whom the institution has a customer relationship or pertains to the customers of other financial institutions that have provided such information to that institution.

<sup>1</sup> This Guidance is being jointly issued by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

<sup>2</sup> 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D-2 and part 225, app. F (Board); 12 CFR part 364, app. B (FDIC); and 12 CFR part 570, app. B (OTS).