DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

Docket No. 03-18

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

No. 03-35

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Docket No. OP-1155

FEDERAL DEPOSIT INSURANCE CORPORATION

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

AGENCIES: Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); and Office of Thrift Supervision, Treasury (OTS).[1]

ACTION: Notice and request for comment.

[1] The National Credit Union Administration (NCUA) participated in the guidance development process and will separately issue comparable proposed guidance.

SUMMARY: The OCC, Board, FDIC, and OTS (the Agencies) are requesting comment on proposed guidance entitled Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice ("the proposed Guidance").

In addition, as part of their continuing efforts to reduce paperwork and respondent burden, the Agencies invite the general public and other Federal agencies to take this opportunity to comment on a proposed information collection, as required by the Paperwork Reduction Act of 1995 (44 U.S.C. chapter 35).

DATES: Comments must be submitted on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Interested parties are invited to submit written comments to:

Office of the Comptroller of the Currency: Public Information Room, Office of the Comptroller of the Currency, 250 E Street, SW, Mail stop 1-5, Washington, DC 20219, Attention: Docket No. 03-18, Fax number (202) 874-4448 or e-mail address: *regs.comments@occ.treas.gov.* Due to delays in the delivery of paper mail in the Washington area, commenters are encouraged to submit their comments by fax or email. Comments may be inspected and photocopied at the OCC's Public Information Room, 250 E Street, SW, Washington, DC. You can make an appointment to inspect the comments by calling (202) 874-5043.

Board of Governors of the Federal Reserve System: Comments should refer to Docket No. OP-1155 and may be mailed to Ms. Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW, Washington, DC 20551. However, because paper mail in the Washington area and at the Board of Governors is subject to delay, please consider submitting your comments by e-mail to *regs.comments@federalreserve.gov*, or faxing them to the Office of the Secretary at (202) 452-3819 or (202) 452-3102. Members of the public may inspect comments in Room MP-500 between 9 a.m. and 5 p.m. on weekdays pursuant to 12 CFR 261.12, except as provided in 12 CFR 261.14, of the Board's Rules Regarding Availability of Information, 12 CFR sections 261.12 and 261.14.

Federal Deposit Insurance Corporation: Send written comments to Robert E. Feldman, Executive Secretary, Attention: Comments/OES, Federal Deposit Insurance Corporation, 550 17th Street, NW, Washington, DC 20429. Comments also may be mailed electronically to *comments@fdic.gov*. Comments may be hand delivered to the guard station at the rear of the 17th Street building (located on F Street) on business days between 7 a.m. and 5 p.m.; Fax Number (202) 898-3838. Comments may be inspected and photocopied in the FDIC Public Information Center, Room 100, 801 17th Street, NW, Washington, DC 20429, between 9 a.m. and 5 p.m. on business days.

Office of Thrift Supervision: Comments may be sent to Regulation Comments, Chief Counsel's Office, Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552, Attention: No.2003-35; FAX number (202) 906-6518, Attention: No. 2003-____;

or e-mail address regs.comments@ots.treas.gov, Attention: No. 2003-____, and include your name and telephone number. Comments may also be hand delivered to the Guard's Desk, East Lobby Entrance, 1700 G Street, NW, from 9:00a.m. to 4:00 p.m. on business days, Attention: Regulation Comments, Chief Counsel's Office, No. 2003-____. Commenters should be aware that there have been unpredictable and lengthy delays in postal deliveries to the Washington, DC area and may prefer to make their comments via facsimile, e-mail, or hand delivery. OTS will post comments and the related index on the OTS Internet Site at www.ots.treas.gov. In addition, you may inspect comments at the Public Reading Room, 1700 G Street, NW, by appointment. To make an appointment for access, you may call (202) 906-5922, send an e-mail to public.info@ots.treas.gov, or send a facsimile transmission to (202) 906-7555. (Please identify the materials you would like to inspect to assist us in serving you.) We schedule appointments on business days between 10:00a.m. and 4:00p.m. In most cases, appointments will be available the business day after the date we receive a request.

FOR FURTHER INFORMATION CONTACT:

OCC: Aida Plaza Carter, Director, Bank Information Technology Operations Division, (202) 874-4740; Clifford A. Wilke, Director, Bank Technology Division, (202) 874-5920; Amy Friend, Assistant Chief Counsel, (202) 874-5200; or Deborah Katz, Senior Attorney, Legislative and Regulatory Activities Division, (202) 874-5090.

Board: Donna L. Parker, Supervisory Financial Analyst, Division of Banking Supervision & Regulation, (202) 452-2614; Thomas E. Scanlon, Counsel, Legal Division, (202) 452-3594; or Joshua H. Kaplan, Attorney, Legal Division, (202) 452-2249.

FDIC: Jeffrey M. Kopchik, Senior Policy Analyst, Division of Supervision and Consumer Protection, (202) 898-3872; Patricia I. Cashman, Senior Policy Analyst, Division of Supervision and Consumer Protection, (202) 898-6534; or Robert A. Patrick, Counsel, Legal Division, (202) 898-3757.

OTS: Robert Engebreth, Director, Technology Risk Management, (202) 906-5631; Lewis C. Angel, Senior Project Manager, Technology Risk Management, (202) 906-5645; Elizabeth Baltierra, Program Analyst (Compliance), Compliance Policy, (202) 906-6540; or Paul Robin, Special Counsel, Regulations and Legislation Division, (202) 906-6648.

SUPPLEMENTARY INFORMATION:

I. Background

The Agencies have published Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Security Guidelines").[2] These Security Guidelines were published to fulfill a requirement in § 501(b) of the Gramm-Leach-Bliley Act in which Congress directed the Agencies to establish standards for financial institutions 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.[3]

Among other things, the Security Guidelines direct financial institutions to: (1) identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and (3) assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.[4]

This proposed Guidance, published as an Appendix to this notice, interprets § 501(b) of

[2] 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).

[3] 15 U.S.C. 6805(b).

[4] Security Guidelines, Paragraph III.B.2.

the Gramm-Leach-Bliley Act and the provisions of the Security Guidelines noted above.[5] It describes the Agencies' expectations that every financial institution develop a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of customer information maintained by the financial institution or its service provider. The proposed Guidance further describes the components of a response program, which includes procedures for notifying customers about incidents of unauthorized access to customer information that could result in substantial harm or inconvenience to the customer. The proposed Guidance provides that a financial institution is expected to expeditiously implement its response program to address incidents of unauthorized access to or use of customer information. A response program should contain 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 use of customer information, including shutting down particular applications

[5] The Agencies may treat an institution's failure to implement final Guidance issued as a violation of the Security Guidelines.

or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls; and

D. Address and mitigate harm to individual customers.

The proposed Guidance describes the following corrective measures a financial institution should include as a part of its response program in order to effectively address and mitigate harm to individual customers.

A. Flag Accounts -- The institution should identify accounts of customers whose information may have been compromised, monitor those accounts for unusual activity, and initiate appropriate controls to prevent the unauthorized withdrawal or transfer of funds from customer accounts.

B. Secure Accounts -- The institution should secure all accounts associated with the customer information that has been the subject of unauthorized access or use.

C. Customer Notice and Assistance -- The institution should, under certain circumstances, notify affected customers when *sensitive customer information* about them is the subject of unauthorized access. Where the institution can specifically identify affected customers from its logs, notification may be limited to those persons only.

Otherwise, the institution should notify each customer in those groups likely to be affected.

The proposed Guidance provides that a financial institution should notify each affected customer when it becomes aware of unauthorized access to *sensitive customer information*, unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur, and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers' accounts for unusual or suspicious activity. For the purposes of the proposed Guidance, the Agencies define *sensitive customer information* to mean a customer's social security number, personal identification number (PIN), password, or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number. *Sensitive customer information* would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such as user name and password.

Under the Security Guidelines, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. The Agencies believe that substantial harm or inconvenience is most likely to result from the improper access to and use of *sensitive customer information*. Accordingly, the proposed Guidance requires notice to mitigate or prevent substantial harm or inconvenience to a customer.

The Agencies note that the response program required under the proposed Guidance must address incidents involving the unauthorized access to or use of any form of customer information. However, the customer notice requirement applies *only* to security breaches involving *sensitive customer information*.

The proposed Guidance provides several examples the Agencies believe typify situations in which customer notification is required and those when it is not. As in other circumstances, the Agencies also expect financial institutions to notify customers upon the direction of the institution's primary federal regulator.

The proposed Guidance discusses the content and delivery of customer notices. The notice should include a general description of the incident, and provide information to assist customers in mitigating potential harm, including a customer service number, steps customers can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

In addition, institutions are expected to inform each customer about the availability of the Federal Trade Commission's ("FTC") online guidance regarding measures to protect against identity theft and to encourage the customer to report any suspected incidents of identity theft to the FTC. Further, institutions should provide the FTC's Web site address and telephone number for purposes of obtaining the guidance and reporting suspected

incidents of identity theft. Currently, the Web site address is www.ftc.gov/idtheft, and the toll free number for the identity theft hotline is 1-877-IDTHEFT.

The proposed Guidance also describes other forms of assistance that financial institutions have offered to their customers in incidents of this type. Financial institutions may wish to offer such forms of assistance to their customers and describe them in the customer notice.

II. Request for Comments

The Agencies invite comment on all aspects of the proposed Guidance, including each component of the response program described in Paragraph II. of the proposed Guidance. Please consider the following questions in formulating your comments:

Should any component of the response program be clarified in some way and, if so, how?

- Are there additional components that should be included in a response program to address incidents involving unauthorized access to or use of customer information? If so, please describe the component, and the reasons that support it.

- Should each component of the response program be retained? If not, which components should be deleted and why?

- In preparing the proposed Guidance, the Agencies have attempted to identify a standard that will lead to customer notice when appropriate. The Agencies recognize that there is a spectrum of alternatives for developing a requirement to notify customers. On one side of the spectrum is a standard that would require a financial institution to notify its customers every time the mere possibility of misuse of customer information arises. On the other side is a standard that would require an institution to notify its customers only when it becomes aware of an incident involving unauthorized access to customer information and, based on unusual activity in customers' accounts or other indicia of identity theft, knows that the information is being misused. The Agencies propose a standard that lies in the middle of this spectrum. The Agencies believe that no useful purpose would be served if notices were sent due to the mere possibility of misuse of some customer information because, in general, the notices should alert customers to those situations where enhanced vigilance is necessary to protect against fraud or identity theft. Rather, the Agencies believe that notice to customers should be required in a narrower range of instances involving the unauthorized access to *sensitive customer information*. The standard proposed here would require a financial institution to send notice to each affected customer when the institution becomes aware of an incident of unauthorized access to *sensitive customer information*, unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur

and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers' accounts for unusual or suspicious activity. The Agencies invite comment on whether this is the appropriate standard for requiring customer notice. For commenters who believe that this standard is inappropriate, the Agencies request that these commenters state specifically their reasoning and offer alternative thresholds for requiring customer notice.

- The proposed Guidance defines *sensitive customer information* as a social security number, a personal identification number (PIN), password, or an account number in conjunction with a personal identifier. *Sensitive customer information* would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such as user name and password. The Agencies request comment on which, if any, additional types of information should be included in this definition, such as mother's maiden name or driver's license number.
- The Agencies invite comment on the potential burden associated with the customer notice provisions. For example, what is the anticipated burden that may arise from the questions posed by those customers who receive the notices? Should the Agencies consider how the burden may vary depending upon the size and complexity of the institution?

- As part of the response program, the Agencies describe certain corrective measures that an institution should take once an incident of unauthorized access occurs. One such measure is to "secure accounts." Is the discussion of securing accounts sufficiently clear to enable institutions to know what is expected of them when instances of unauthorized access occur? To what extent would contracts between financial institutions and service providers need to be modified, if at all, to comply with the proposed Guidance? How much burden, if any, will the Guidance impose on service providers?

- The Agencies also invite comment on whether the proposed standard should be modified to apply to other extraordinary circumstances that compel an institution to conclude that unauthorized access to information, other than *sensitive customer information*, likely will result in substantial harm or inconvenience to the affected customers.

- The proposed Guidance includes examples of circumstances in which customer notice would be expected and those when it would not. Please comment on whether the examples in the proposed Guidance should be modified or supplemented and provide your rationale.

III. Paperwork Reduction Act

A. Request for Comment on Proposed Information Collection

In accordance with the requirements of the Paperwork Reduction Act of 1995, the Agencies may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number. The Agencies are requesting comment on a proposed information collection. The Agencies also give notice that, at the end of the comment period, the proposed collections of information, along with an analysis of the comments and recommendations received, will be submitted to OMB for review and approval.

Comments are invited on:

(a) Whether the collection of information is necessary for the proper performance of the Agency's functions, including whether the information has practical utility;

(b) The accuracy of the estimates of the burden of the information collection, including the validity of the methodology and assumptions used;

(c) Ways to enhance the quality, utility, and clarity of the information to be collected;

(d) Ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology; and

(e) Estimates of capital or start up costs and costs of operation, maintenance, and purchase of services to provide information.

At the end of the comment period, the comments and recommendations received will be analyzed to determine the extent to which the information collections should be modified prior to submission to OMB for review and approval. The comments will also be summarized or included in the Agencies' requests to OMB for approval of the collections. All comments will become a matter of public record.

Comments should be addressed to:

OCC: Public Information Room, Office of the Comptroller of the Currency, 250 E Street, SW, Mail stop 1-5, Attention: Docket 03-18, Washington, DC 20219; fax number (202) 874-4448; Internet address: *regs.comments@occ.treas.gov*. Due to delays in paper

mail delivery in the Washington area, commenters are encouraged to submit their comments by fax or e-mail. You can make an appointment to inspect the comments at the Public Information Room by calling (202) 874-5043.

Board: Comments should refer to Docket No. OP-1155 and may be mailed to Ms. Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW, Washington, DC 20551. However, because paper mail in the Washington area and at the Board of Governors is subject to delay, please consider submitting your comments by e-mail to *regs.comments@federalreserve.gov*, or faxing them to the Office of the Secretary at (202) 452-3819 or (202) 452-3102. Members of the public may inspect comments in Room MP-500 between 9 a.m. and 5 p.m. on weekdays pursuant to 12 CFR section 261.12, except as provided in 12 CFR section 261.14, of the Board's Rules Regarding Availability of Information, 12 CFR sections 261.12 and 261.14.

FDIC: Steven F. Hanft, Legal Division (Consumer and Compliance Unit), Room MB-3064, Federal Deposit Insurance Corporation, 550 17th Street, NW, Washington, DC 20429. All comments should refer to the title of the proposed collection. Comments may be hand-delivered to the guard station at the rear of the 17th Street Building (located on F Street), on business days between 7 a.m. and 5 p.m., Attention: Comments, Federal Deposit Insurance Corporation, 550 17th Street, NW, Washington, DC 20429.

OTS: Information Collection Comments, Chief Counsel's Office, Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552; send a facsimile transmission to (202) 906-6518; or send an e-mail to *infocollection.comments@ots.treas.gov*. OTS will post comments and the related index on the OTS internet site at *www.ots.treas.gov*. In addition, interested persons may inspect the comments at the Public Reading Room, 1700 G Street, NW, by appointment. To make an appointment, call (202) 906-5922, send an e-mail to *publicinfo@ots.treas.gov*, or send a facsimile transmission to (202) 906-7755.

B. Proposed Information Collection

Title of Information Collection: Notice Regarding Unauthorized Access to Customer Information.

Frequency of Response: On occasion.

Affected Public:

OCC: – National banks, District of Columbia banks, and Federal branches and agencies of foreign banks.

Board: – State member banks, bank holding companies, affiliates and certain non-bank subsidiaries of bank holding companies, uninsured state agencies and branches of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and agreement corporations.

FDIC: – Insured nonmember banks, insured state branches of foreign banks, and certain subsidiaries of these entities.

OTS: – Savings associations and certain of their subsidiaries.

Abstract: The proposed 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 proposed Guidance would require financial institutions to: (1) develop notices to customers; (2) determine which customers should receive the notices and send the notices to customers; and (3) ensure that their contracts with their service providers satisfy the proposed Guidance.

Estimated Burden: It is estimated that it will initially take institutions 20 hours (2.5 business days) to develop and produce the notices described in the proposed Guidance and 24 hours per incident (three business days) to determine which customers should receive the notice and notify the customers. For the purposes of this analysis, it is estimated that two percent of supervised institutions will experience an incident of unauthorized access to customer information on an annual basis, resulting in customer notification.[6]

Thus, the burden associated with this collection of information may be summarized as follows. However, the burden estimate does not include time for financial institutions to adjust their contracts with service providers, if needed; nor for service providers to disclose information pursuant to the proposed Guidance.

OCC:

Number of Respondents: 2,200

Estimated Time per Response:

Developing notices: 20 hrs. x 2,200 = 44,000 hours

Notifying customers: 24 hrs. x 44 = 1,056 hours

Total Estimated Annual Burden = 45,056 hours

Board:

[6] This estimate is based upon the Agencies' experience and data gathered by the FDIC on 2,000 institutions that indicates slightly less than one percent of those institutions experienced some form of unauthorized access to customer information during any 12 month period. However, the Agencies are assuming that other incidents of unauthorized access to customer information may have occurred but were not reported.

Number of Respondents: 6,692

Estimated Time per Response:

Developing notices: 20 hrs. x 6,692 = 133,840 hours

Notifying customers: 24 hrs. x 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. x 5,500 = 110,000 hours

Notifying customers: 24 hrs. x 110 = 2,640 hours

Total Estimated Annual Burden: 112,640 hours

OTS:

Number of Respondents: 961.

Estimated Time per Response:

Developing notices: 20 hrs. x 961 = 19,220 hours

Notifying customers: 24 hrs. x 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[7] interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Security Guidelines")[8] 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

[7] 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).

[2] 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).

information.[9] 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;

[9] 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.

- 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.[10]

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,[11] 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

[10] See Security Guidelines Paragraph III.B.

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.[12]

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.[13] 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.[14] In view of these contractual obligations, the service

---

[11] See Security Guidelines Paragraph III.C.

[12] See Security Guidelines Paragraph III.D.

[13] See Security Guidelines Paragraphs II.B. and III.D.

[14] 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,

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.[15]

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

---

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.

[15] 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.

program.[16] Having such a program in place will allow the institution to quickly respond[17] to incidents involving the unauthorized access to or use of customer information in its own customer information systems that could result in substantial harm or inconvenience to a customer. Under the Guidelines, an institution's *customer information systems* consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers.[18]

Timely notification of customers, under the circumstances described below, is important to manage an institution's reputation risk. Effective notice may reduce legal risk, assist in maintaining good customer relations, and enable the institution's customers to take steps to protect themselves against the consequences of identity theft.

A response program should contain the following components:

---

[16] See FFIEC Information Security Booklet, Dec. 2002; Federal Reserve SR 97-32, Sound Practice Guidance for Information Security for Networks, Dec. 4, 1997; OCC Bulletin 2000-14, "Infrastructure Threats – Intrusion Risks" (May 15, 2000); OTS CEO Memorandum 109, Transactional Web Sites, June 10, 1999; CEO Memorandum 70, Statement on On-Line Personal Computer Banking, June 23, 1997; CEO Memorandum 59, Risk Management of Client/Server Systems, Oct. 24, 1996, for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

[17] Financial institutions are expected to provide employees with the training necessary to understand their roles and responsibilities in order to expeditiously implement the institution's response program to address incidents of unauthorized access to and use of customer information.

[18] See Security Guidelines Paragraph I.C.f.

A. Assess the Situation. – The institution should assess the nature and scope of the incident, and identify what customer information systems and types of customer information have been accessed or misused.

B. Notify Regulatory and Law Enforcement Agencies – The institution should promptly notify its primary Federal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers.

An institution also should file a Suspicious Activity Report ("SAR"), if required, in accordance with the applicable SAR regulations[19] and Agency guidance.[20] Consistent with the Agencies' SAR regulations, in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, the institution should immediately notify, by telephone, appropriate law enforcement authorities and its primary regulator, in addition to filing a timely SAR.

---

[19] 12 CFR 21.11 (national banks, federal branches and agencies); 12 CFR 208.62 (state member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured state branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); 12 CFR part 353 (state non-member banks); and 12 CFR part 563 (savings associations).

[20] National banks must file SARs in connection with computer intrusions and other computer crimes. See OCC Bulletin 2000-14, "Infrastructure Threats – Intrusion Risks" (May 15, 2000); Advisory Letter 97-9, "Reporting Computer Related Crimes" (November 19, 1997) (general guidance still applicable though instructions for new SAR form published in 65 FR 1229, 1230 (January 7, 2000)). See also Federal Reserve SR 01-11, Identity Theft and Pretext Calling, Apr. 26, 2001; SR 97-28, Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions, Nov. 6, 1997; FDIC FIL 48-2000, Suspicious Activity Reports, July 14, 2000; FIL 47-97, Preparation of Suspicious Activity Reports, May 6, 1997; OTS CEO Memorandum 139, Identity Theft and Pretext Calling, May 4, 2001; CEO Memorandum 126, New Suspicious Activity Report Form, July 5, 2000.

C. Contain and Control the Situation – The financial institution should take measures to contain and control the incident to prevent further unauthorized access to or use of customer information, while preserving records and other evidence.[21] Depending upon the particular facts and circumstances of the incident, these measures could include, in connection with computer intrusions: (i) shutting down applications or third party connections; (ii) reconfiguring firewalls in cases of unauthorized electronic intrusion; (iii) ensuring that all known vulnerabilities in the financial institution's computer systems have been addressed; (iv) changing computer access codes; (v) modifying physical access controls; and (vi) placing additional controls on service provider arrangements.

D. Corrective measures – Once an institution understands the scope of the incident and has taken steps to contain and control the situation, it should take measures to address and mitigate the harm to individual customers. For example, the institution should take the following measures:

1. Flag Accounts – The institution should immediately begin identifying and monitoring the accounts of those customers whose information may have been accessed or misused. In particular, the institution should provide staff with instructions regarding the recording and reporting of any unusual activity, and if indicated given the facts of a particular incident, implement controls to prevent the unauthorized withdrawal or transfer of funds from customer accounts.

---

[21] See FFIEC Information Security Booklet, Dec. 2002, pp. 68-74.

2. Secure Accounts – When a checking, savings, or other deposit account number, debit or credit card account number, personal identification number (PIN), password, or other unique identifier has been accessed or misused, the financial institution should secure the account, and all other accounts and bank services that can be accessed using the same account number or name and password combination until such time as the financial institution and the customer agree on a course of action.[22]

3. Customer Notice and Assistance – Under the Security Guidelines, financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. An institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so. Under the circumstances described in Paragraph III., the institution should notify and offer assistance to customers whose information was the subject of the incident.[23] If the institution is able to determine from its logs or other data precisely which customers' information was accessed or misused, it may restrict its notification to those individuals. However, if the institution cannot identify precisely which customers are affected, it should notify each customer in groups likely to have been affected, such as each customer whose information is stored in the group of files in question.

---

[22] The institution should also consider the use of new account numbers and steps to ensure that customers do not reuse the same or a similar personal identification number.

[23] The institution should, therefore, ensure that a sufficient number of appropriately trained employees are available to answer customer inquiries and provide assistance.

a. Delivery of Customer Notice – Customer notice should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the customer is likely to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or for those customers who conduct transactions electronically, using electronic notice.

b. Content of Customer Notice --The notice should describe the incident in general terms and the customer's information that was the subject of unauthorized access or use. It should also include a number that customers can call for further information and assistance. The notice also should remind customers of the need to remain vigilant, over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft.

Key Elements: In addition, the notice should:

- Inform affected customers that the institution will assist the customer to correct and update information in any consumer report relating to the customer, as required by the Fair Credit Reporting Act;

- Recommend that the customer notify each nationwide credit reporting agency to place a fraud alert[24] in the customer's consumer reports;

- Recommend that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

- Inform the customer of the right to obtain a credit report free of charge, if the customer has reason to believe that the file at the consumer reporting agency contains inaccurate information due to fraud, together with contact information regarding the nationwide credit reporting agencies; and

- Inform the customer about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft, and encourage the customer to report any incidents of identity theft to the FTC. The notice should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.[25]

[24] A fraud alert will put the customer's creditors on notice that the customer may be a victim of fraud.

[19] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *www.ftc.gov/idtheft* and 1-877-IDTHEFT.

Optional Element: Institutions also may wish to provide customers with the following additional assistance that other institutions have offered under these circumstances:

- Provide a toll-free telephone number that customers can call for assistance;

- Offer to assist the customer in notifying the nationwide credit reporting agencies of the incident and in placing a fraud alert in the customer's consumer reports; and

- Inform the customer about subscription services that provide notification anytime there is a request for the customer's credit report or offer to subscribe the customer to this service, free of charge, for a period of time.

The institution may also wish to include with the notice a brochure regarding steps a consumer can take to protect against identity theft, prepared by the Agencies that can be downloaded from the Internet.[26]

III. Circumstances for Customer Notice

Standard for Providing Notice

An institution should notify affected customers whenever it becomes aware of unauthorized access to *sensitive customer information* unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers, including by monitoring affected customers' accounts for unusual or suspicious activity.

Sensitive Customer Information

Under the Guidelines, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to *sensitive customer information* because this type of information is easily misused, as in the commission of identity theft. For purposes of this Guidance, *sensitive customer information* means a customer's social security number, personal identification number, password or account number, in conjunction with a personal identifier such as the customer's name, address, or telephone number. *Sensitive customer information* would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such as user name and password. Therefore, institutions are expected to notify affected customers when *sensitive customer information* has been improperly accessed, unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is

[26] *www.occ.treas.gov/idtheft.pdf; www.federalreserve.gov/consumers.htm; www.fdic.gov/consumers/consumer/news/cnsum00/idthft.html;www.ots.treas.gov/docs/25139.pdf.*

unlikely to occur and takes appropriate steps to safeguard the interests of affected customers.

Examples of When Notice Should be Given

An institution should notify affected customers when it is aware of the following incidents unless the institution, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers.

- An employee of the institution has obtained unauthorized access to *sensitive customer information* maintained in either paper or electronic form;

- A cyber intruder has broken into an institution's unencrypted database that contains *sensitive customer information*;

- Computer equipment such as a laptop computer, floppy disk, CD-ROM, or other electronic media containing *sensitive customer information* has been lost or stolen;

- An institution has not properly disposed of customer records containing *sensitive customer information*; or

- The institution's third party service provider has experienced any of the incidents described above, in connection with the institution's *sensitive customer information*.

Examples of When Notice is Not Expected

An institution is not expected to give notice when it becomes aware of an incident of unauthorized access to customer information, and the institution, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers. For example, an institution would not need to notify affected customers in connection with the following incidents:

- The institution is able to retrieve *sensitive customer information* that has been stolen, and reasonably concludes, based upon its investigation of the incident, that it has done so before the information has been copied, misused or transferred to another person who could misuse it;

- The institution determines that *sensitive customer information* was improperly disposed of, but can establish that the information was not retrieved or used before it was destroyed;

- A hacker accessed files that contain only customer names and addresses; or

- A laptop computer containing *sensitive customer information* is lost, but the data is encrypted and may only be accessed with a secure token or similarly secure access device.

[THIS SIGNATURE PAGE PERTAINS TO THE NOTICE AND REQUEST FOR COMMENT TITLED, "INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE"]

Dated: _____

_____

Mark J. Tenhundfeld
Assistant Director
Office of the Comptroller of the Currency.

[THIS SIGNATURE PAGE PERTAINS TO THE NOTICE AND REQUEST FOR COMMENT TITLED, "INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE"]

By the Board of Governors of the Federal Reserve System on _____, 2003.

_____

Jennifer J. Johnson
Secretary of the Board

[THIS SIGNATURE PAGE PERTAINS TO THE NOTICE AND REQUEST FOR COMMENT TITLED, "INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE"]

Dated: _____

_____

Michael J. Zamorski
Director, Division of Supervision and
Consumer Protection
Federal Deposit Insurance Corporation.

[THIS SIGNATURE PAGE PERTAINS TO THE NOTICE AND REQUEST FOR COMMENT TITLED, "INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE"]

Dated: _____

BY THE OFFICE OF THRIFT SUPERVISION

_____

James E. Gilleran
Director