Office of Thrift Supervision
Department of the Treasury *Managing Director, Examinations, Supervision, and Consumer Protection*
1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

March 30, 2005

MEMORANDUM FOR: CHIEF EXECUTIVE OFFICERS

FROM: Scott M. Albinson

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

The Office of Thrift Supervision (OTS), along with the other federal banking regulatory agencies, has issued the attached *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*.

OTS published the new guidance as Supplement A to 12 CFR part 570, appendix B, *Interagency Guidelines Establishing Information Security Standards* (Guidelines). This guidance interprets the Guidelines and states that you should develop and implement a response program to address security breaches involving customer information. The response program should include procedures to notify your customers about incidents of unauthorized access to their information that could result in substantial harm or inconvenience to them.

The new guidance provides that when you become aware of an incident of unauthorized access to sensitive customer information, you should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If you determine that misuse of information about a customer has occurred or is reasonably possible, you should notify the affected customer as soon as possible. However, notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation. You should notify your OTS regional office of a security breach involving sensitive customer information whether or not you notify your customers.

In issuing this guidance, OTS also made a conforming change to the *Protection of Customer Information* rule at 12 CFR 568.5. The change clarifies that Supplement A to the Guidelines is intended as interpretive guidance.

Questions regarding this guidance should be directed to Lewis C. Angel, Technology Program Manager, Technology Risk Management, (202) 906-5645. For further information on technology risk management issues, see OTS's Internet site at www.ots.treas.gov/supervision/issuances.

Attachment

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

I. Background

This Guidance[1] interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA") and the Interagency Guidelines Establishing Information Security Standards (the "Security Guidelines")[2] and describes response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

The scope of, and definitions of terms used in, this Guidance are identical to those of the Security Guidelines. For example, the term "customer information" is the same term used in the Security Guidelines, and means any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form, maintained by or on behalf of the institution.

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. 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:

[1] 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). This document renames the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" as the "Interagency Guidelines Establishing Information Security Standards."

- 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.[3]

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,[4] 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 financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.[5]

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.[6]

II. Response Program

Millions of Americans, throughout the country, have been victims of identity theft.[7] Identity thieves misuse personal information they obtain from a number of sources, including financial

[3] See Security Guidelines, III.B.
[4] See Security Guidelines, III.C.
[5] See Security Guidelines, III.C.
[6] See Security Guidelines, II.B. and III.D. Further, 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 Federal Trade Commission ("FTC"), 12 CFR part 314.
[7] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identity theft in 2002. See The Federal Trade Commission, Identity Theft Survey Report, (September 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

institutions, to perpetrate identity theft. Therefore, financial institutions should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information. For example, financial institutions should place access controls on customer information systems and conduct background checks for employees who are authorized to access customer information.[8] However, every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems[9] that occur nonetheless. A response program should be a key part of an institution's information security program.[10] The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to customer information in customer information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in the Guidelines that relate to these arrangements, and with existing guidance on this topic issued by the Agencies,[11] an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

Components of a Response Program

At a minimum, an institution's response program should contain procedures for the following:

- Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
- Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
- Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations,[12] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations

[8] Institutions should also conduct background checks of employees to ensure that the institution does not violate 12 U.S.C. 1829, which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1818(e)(6).

[9] 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. See Security Guidelines, I.C.2.d (I.C.2.c for OTS).

[10] See FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002 available at http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm. 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), for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

[11] See Federal Reserve SR Ltr. 00-04, Outsourcing of Information and Transaction Processing, Feb. 9, 2000; OCC Bulletin 2001-47, "Third-Party Relationships Risk Management Principles," Nov. 1, 2001; FDIC FIL 68-99, Risk Assessment Tools and Practices for Information System Security, July 7, 1999; OTS Thrift Bulletin 82a, Third Party Arrangements, Sept. 1, 2004.

[12] An institution's obligation to file a SAR is set out in the Agencies' SAR regulations and Agency guidance. See 12 CFR 21.11 (national banks, federal branches and agencies); 12 CFR 208.62 (state member banks); 12 CFR

involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
- Taking appropriate steps to contain and control the incident 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;[13] and
- Notifying customers when warranted.

Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's customers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's customers or regulator on its behalf.

III. Customer Notice

Financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. Notifying customers of a security incident involving the unauthorized access or use of the customer's information in accordance with the standard set forth below is a key part of that duty.

Timely notification of customers is important to manage an institution's reputation risk. Effective notice also may reduce an institution's 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. When customer notification is warranted, 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.

Standard for Providing Notice

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

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 563.180 (savings associations). 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; http://www.ots.treas.gov/BSA (for the latest SAR form and filing instructions required by OTS as of July 1, 2003).

[13] See FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002, pp. 68-74.

Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

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 most likely to be misused, as in the commission of identity theft.

For purposes of this Guidance, sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

Affected Customers

If a financial institution, based upon its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the institution determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the institution determines that a group of files has been accessed improperly, but is unable to identify which specific customers' information has been accessed. If the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible, it should notify all customers in the group.

Content of Customer Notice

Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It also should generally describe what the institution has done to protect the customers' information from further unauthorized access. In addition, it should include a telephone number that customers can call for further information and assistance.[14] 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 to the institution.

[14] The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

The notice should include the following additional items, when appropriate:

- A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;
- A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
- A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- An explanation of how the customer may obtain a credit report free of charge; and
- Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and 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.[15]

The Agencies encourage financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

Delivery of Customer Notice

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

[15] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are www.consumer.gov/idtheft and 1-877-IDTHEFT. The institution may also refer customers to any materials developed pursuant to section 151(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).