



OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Response Programs for Unauthorized Access to Customer Information and
Customer Notice: Final Guidance

Description: Interagency Guidance

TO: Chief Executive Officers of All National Banks, Federal Branches and Agencies,
Technology Service Providers, Department and Division Heads, and All Examining
Personnel

The OCC, FRB, FDIC, and OTS are issuing the attached final "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." The guidance was published in the *Federal Register* on March 29, 2005, and became effective upon publication.

The guidance interprets the Interagency Guidelines Establishing Information Security Standards (Security Guidelines)¹ and states that each financial institution should implement a response program to address unauthorized access to customer information maintained by the institution or its service providers. The guidance describes the components that a response program should contain including procedures to notify customers about incidents that involve unauthorized access to *sensitive* customer information.

The guidance provides 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 misuse of its information about a customer has occurred or is reasonably possible, it 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 and provides the institution with a written request for a delay.

Sensitive customer information is defined to mean 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.

¹ This guidance will be published in the Code of Federal Regulations as a supplement to the Security Guidelines that are codified at 12 CFR 30, Appendix B. The Security Guidelines were formerly known as the "Interagency Guidelines Establishing Safeguards for Customer Information."

The guidance states that a financial institution's contract with each 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.

The guidance also provides that a financial institution should notify its primary federal regulator of a security breach involving sensitive customer information, whether or not the institution notifies its customers. A national bank should notify its supervisory office.

When evaluating the adequacy of a national bank's information security program required by the Security Guidelines, the OCC will consider whether the bank has developed and implemented a response program including notification procedures as described in the guidance. The OCC will take into account the good faith efforts made by each bank to develop a response program that is consistent with the guidance, together with all other relevant circumstances. The OCC may treat a bank's failure to implement the final guidance as a violation of the Security Guidelines that are enforceable under the procedures set forth in 12 USC 1831p-1, or as an unsafe and unsound practice under 12 USC 1818.

For questions concerning the guidance, contact Aida Plaza Carter, director for Bank Information Technology Operations at (202) 874-4740; Amy Friend, assistant chief counsel at (202) 874-5200; or Deborah Katz, senior counsel, Legislative and Regulatory Activities Division at (202) 874-5090.

Daniel P. Stipano
Acting Chief Counsel

Emory W. Rushton
Senior Deputy Comptroller and Chief National Bank Examiner

Attachment: [70 FR 15736](#)
[<http://www.occ.treas.gov/fr/fedregister/70fr15736.pdf>]

nationwide consumer reporting agencies. The commenter stated that the nationwide consumer reporting agencies spent approximately \$1.5 million per company, handling approximately 365,000 inquiries from the company's customers.

The final Guidance contains a number of changes that will diminish the costs identified by these commenters. First, the standard for notification in the final Guidance likely will result in fewer notices. In addition, the final Guidance no longer states that all notices should advise customers to contact the nationwide consumer reporting agencies. Therefore, the Agencies' estimates do not factor in the costs to the reporting agencies.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act applies only to rules for which an agency publishes a general notice of proposed rulemaking pursuant to 5 U.S.C. 553(b). See 5 U.S.C. 601(2). As previously noted, a general notice of proposed rulemaking was not published because this final Guidance is a general statement of policy. Thus, the Regulatory Flexibility Act does not apply to the final Guidance.

With respect to OTS's revision to its regulation at 12 CFR 568.5, as noted above, OTS has concluded that there is good cause to dispense with prior notice and comment. Accordingly, OTS has further concluded that the Regulatory Flexibility Act does not apply to this final rule.

C. Executive Order 12866

The OCC and OTS have determined that this final Guidance is not a significant regulatory action under Executive Order 12866. With respect to OTS's revision to its regulation at 12 CFR 568.5, OTS has further determined that this final rule is not a significant regulatory action under Executive Order 12866.

D. Unfunded Mandates Reform Act of 1995

The OCC and OTS have determined that this final Guidance is not a regulatory action that would require an assessment under the Unfunded Mandates Reform Act of 1995 (UMRA), 2 U.S.C. 1531. The final Guidance is a general statement of policy and, therefore, the OCC and OTS have determined that the UMRA does not apply.

With respect to OTS's revision to its regulation at 12 CFR 568.5, as noted above, OTS has concluded that there is good cause to dispense with prior notice and comment. Accordingly, OTS has

concluded that the UMRA does not require an unfunded mandates analysis.

Text of Common Final Guidance

The text of the Agencies' common final Guidance reads as follows:

Supplement A to Appendix _ to Part _ — Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

I. Background

This Guidance¹ 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.

A. 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:

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

B. Risk Assessment and Controls

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

- a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration,

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). The "Interagency Guidelines Establishing Information Security Standards" were formerly known as "The Interagency Guidelines Establishing Standards for Safeguarding Customer Information."

or destruction of customer information or customer information systems;

- b. The likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and
- c. The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.³

2. 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:

- a. 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;
- b. Background checks for employees with responsibilities for access to customer information; and
- c. 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

C. 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 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

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/synovate-report.pdf>.

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 systems⁹ 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.

A. Components of a Response Program

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

- a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
- b. 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:

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/ffiecinfo/infobase/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 Third Bulletin 82a, Third Party Arrangements, Sept. 1, 2004.

c. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations,¹² notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. 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

e. Notifying customers when warranted.

2. 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

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 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 5, 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.

institution believes that it may be potentially embarrassed or inconvenienced by doing so.

A. 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. 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.

1. 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.

2. 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.

B. Content of Customer Notice

1. 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

