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) 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
The commenter stated that the Regulatency Flexibility Act does not apply to this final Guidance is not a significant regulatory action 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. * 

Section 501(b) of the GLBA required the Agencies to establish appropriate standards for financial institutions subject to their jurisdiction to implement safeguards to protect the security and confidentiality of customer information. Accordingly, the Agencies issued Security Guidelines for financial institutions to have an information security program designed to:

1. The Security Guidelines direct every financial institution to address 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, 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. ¹

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,¹ and adopt those that are appropriate for the institution, including:

   a. Background checks for employees with responsibilities for access to customer information;
   b. 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.⁶

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. * 

II. Response Program

Millions of Americans, throughout the country, have been victims of identity theft.² 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

*See Security Guidelines, III.B.
¹ See Security Guidelines, III.C.
² See Security Guidelines, III.C.
³ See Security Guidelines, 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.
institutions should place access controls on customer information systems and conduct background checks for employees who are authorized to access customer information. 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 that occur nonetheless. A response program should be a key part of an institution's information security program. 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, 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;
   c. Notifying the institution's customers as soon as possible when the institution determines that misuse of the information has occurred or is reasonably likely to occur;
   d. Notifying the institution's customers when warranted.
   e. Assessing the nature and scope of an incident involving unauthorized access to or use of sensitive customer information, as defined below; and
   f. Notifying the institution's customers as soon as possible when the institution determines that misuse of the information has occurred or is reasonably likely to occur.

2. For purposes of this Guidance, sensitive customer information means any 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, 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.

3. 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.

4. 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 customer information, as defined below;

2. Customer notification is warranted. An institution may not rely on a prohibition order under 12 U.S.C. 1818(e)(2) or a rule under 12 U.S.C. 1829, "which prohibits an unauthorized access or use of customer information involves customer information maintained by an institution's service providers. It is the responsibility of the financial institution to notify the 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 unauthorized access to 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 inconvenient 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 provide a basis for determining whether the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a social security number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account, such as user name and password or password and account number, or a personal identification number or password that would permit access to the customer's account, such as user name and password or password and account number.

B. Affected Customers

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.

C. Content of Customer Notice

1. Customer notification 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. The notice should generally describe what the institution has done to protect the information, as defined below;

2. The notice should include:
   a. The type of security incident that occurred;
   b. The date and location of the incident;
   c. The number of customers affected;
   d. The steps the institution has taken to address the incident;
   e. The steps customers should take to protect against the consequences of identity theft, such as user name and password or password and account number,
   f. The steps customers should take to protect against the consequences of identity theft, such as user name and password or password and account number,
   g. The steps customers should take to protect against the consequences of identity theft, such as user name and password or password and account number.
   h. The steps customers should take to protect against the consequences of identity theft, such as user name and password or password and account number.
customers' information from further unauthorized access. In addition, it should include a telephone 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 to the institution. The notice should include the following additional items, when appropriate:

a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution.

b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer’s consumer reports.

c. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer’s consumer reports.

d. An explanation of how the customer may obtain a credit report free of charge from the nationwide consumer credit reporting agency and have information relating to fraudulent transactions deleted; and

e. Information about the availability of the FTC’s online guidance regarding S I(PS and the FTC’s Web site address and toll-free telephone number that customers should include when contacting the FTC to report any incidents of identity theft.

The notice should encourage the customer to the FTC, and should provide the customer with the FTC’s Web site address and toll-free telephone number that customers should include when contacting the FTC to report any incidents of identity theft. The notice should also remind customers to include the following additional information:

1. 12 CFR Part 30
   Banks, banking, Consumer protection, National banks, Privacy, Reporting and recordkeeping requirements.

2. 12 CFR Part 208
   Banks, banking, Consumer protection, Information, Privacy, Reporting and recordkeeping requirements.

3. 12 CFR Part 223
   Banks, banking, Holding companies, Reporting and recordkeeping requirements.

4. 12 CFR Part 364
   Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and Soundness.

5. 12 CFR Part 570
   Accounting, Administrative practice and procedure, Bank deposit insurance, Consumer protection, Holding companies, Privacy, Reporting and recordkeeping requirements, Safety and Soundness, Savings associations.

6. 12 CFR Part 770
   Accounting, Administrative practice and procedure, Bank deposit insurance, Consumer protection, Holding companies, Privacy, Reporting and recordkeeping requirements, Safety and Soundness, Savings associations.

C. 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.

Adoption of Final Guidance

The agency-specific adoption of the common final Guidance, which appears at the end of the common preamble, follows:

List of Subjects
12 CFR Part 30
Banks, banking, Consumer protection, National banks, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 208
Banks, banking, Consumer protection, Information, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 223
Banks, banking, Holding companies, Reporting and recordkeeping requirements.

12 CFR Part 364
Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and Soundness.

12 CFR Part 570
Accounting, Administrative practice and procedure, Bank deposit insurance, Consumer protection, Holding companies, Privacy, Reporting and recordkeeping requirements, Safety and Soundness, Savings associations.

12 CFR Part 770
Accounting, Administrative practice and procedure, Bank deposit insurance, Consumer protection, Holding companies, Privacy, Reporting and recordkeeping requirements, Safety and Soundness, Savings associations.

Government

PART 30—SAFETY AND SOUNDNESS STANDARDS

1. The authority citation for 12 CFR part 30 continues to read as follows:


2. Revise the heading of Appendix B to read as follows:

   Appendix B to Part 30—Interagency Guidelines Establishing Information Security Standards

3. Amend Appendix B to part 30 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.

Dated: March 8, 2005.

Julie L. Williams,
Acting Comptroller of the Currency.

FEDERAL RESERVE SYSTEM
12 CFR CHAPTER II
Authority and Issuance

1. The authority citation for 12 CFR part 208 continues to read as follows:


2. Revise the heading of Appendix D–Z to read as follows:

   Appendix D–Z to Part 208—Interagency Guidelines Establishing Information Security Standards

3. Amend Appendix D–Z to part 208 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.

PART 225—BANK HOLDING COMPANIES AND CHANGE IN BANK CONTROL (REGULATION Y)

4. The authority citation for 12 CFR part 225 is revised to read as follows:


5. Revise the heading of Appendix F to read as follows:

   Appendix F to Part 225—Interagency Guidelines Establishing Information Security Standards

6. Amend Appendix F to part 225 by adding a new Supplement A to the end of the appendix to read as set forth at the end of the common preamble.