DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR part 30

[Docket No. 05-xx]

RIN 1557-AC92

FEDERAL RESERVE SYSTEM

12 CFR parts 208 and 225

[Docket No. OP-1155]

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR part 364

RIN 3064-AC87

DEPARTMENT OF THE TREASURY

Office of Thrift Supervision

12 CFR parts 568 and 570

No. 2005-11

RIN 1550-AB97

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); Office of Thrift Supervision, Treasury (OTS).

ACTION: Interpretive guidance and OTS final rule.

SUMMARY: The OCC, Board, FDIC, and OTS (the Agencies) are publishing an interpretation of the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines Establishing Information Security Standards (Security Guidelines).[1] This interpretive guidance, titled "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" (final Guidance), is being published as a supplement to the Security Guidelines in the Code of Federal Regulations in order to make the interpretation more accessible to financial institutions and to the general public. The final Guidance will clarify the responsibilities of financial institutions under applicable Federal law. OTS is also making a conforming, technical change to its Security Procedures Rule.

DATE: [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT:

OCC: Aida Plaza Carter, Director, Bank Information Technology, (202) 874-4740; Amy Friend, Assistant Chief Counsel, (202) 874-5200; or Deborah Katz, Senior Counsel, Legislative and Regulatory Activities Division, (202) 874-5090, at 250 E Street, SW., Washington, DC 20219.

Board: Donna L. Parker, Supervisory Financial Analyst, Division of Banking Supervision & Regulation, (202) 452-2614; or Joshua H. Kaplan, Attorney, Legal Division, (202) 452-2249, at 20th and C Streets, NW., Washington, DC 20551.

FDIC: Jeffrey M. Kopchik, Senior Policy Analyst, Division of Supervision and Consumer Protection, (202) 898-3872; Kathryn M. Weatherby, Examiner Specialist, Division of Supervision and Consumer Protection, (202) 898-6793; or Robert A. Patrick, Counsel, Legal Division, (202) 898-3757, at 550 17th Street, NW., Washington, DC 20429.

[1] This document renames the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" as the "Interagency Guidelines Establishing Information Security Standards." Therefore, all other references in the Agencies' regulations to the former title of the Security Guidelines shall be read to refer to the new title.

OTS: Lewis C. Angel, Program Manager, (202) 906-5645; Glenn Gimble, Senior Project Manager, Consumer Protection and Specialized Programs, (202) 906-7158; or Richard Bennett, Counsel, Regulations and Legislation Division, (202) 906-7409, at 1700 G Street, NW., Washington, DC 20552.

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

I. Introduction

The Agencies are jointly issuing final Guidance that interprets the requirements of section 501(b) of the GLBA, 15 U.S.C. 6801, and the Security Guidelines[2] to include the development and implementation of a response program to address unauthorized access to, or use of customer information that could result in substantial harm or inconvenience to a customer. The Guidance describes the appropriate elements of a financial institution's response program, including customer notification procedures.

Section 501(b) required the Agencies to establish standards for financial institutions

relating to administrative, technical, and physical safeguards 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.

On February 1, 2001, the Agencies issued the Security Guidelines as required by section 501(b) (66 FR 8616). 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.[3]

To address the need for additional interpretive guidance regarding section 501(b) and the Security Guidelines, on August 12, 2003, the Agencies published proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (proposed Guidance) in the **Federal Register** (68 FR 47954). This proposed Guidance made clear that the Agencies expect a financial institution's information security program, required under the Security Guidelines, to include a response program.

The Agencies were interested in the public's views on the proposed Guidance and accordingly published it for comment.[4] The Agencies have used these comments to assess the

---

[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). In this Guidance, citations to the Agencies' Security Guidelines refer only to the appropriate paragraph number, as these numbers are common to each of the Guidelines.

[3] Security Guidelines, III.B.2.

[4] Under the Administrative Procedure Act (APA), an agency may dispense with public notice and an opportunity to comment for general statements of policy. 5 U.S.C. 553(b)(A). Therefore, notice and comment were not required under the APA for this final Guidance. OTS has concluded that notice and comment were also not required under the APA for its conforming and technical change as discussed in Part VI of this Supplementary Information.

impact of the proposed Guidance, and to address the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

II. Overview of Comments Received

The Agencies invited comment on all aspects of the proposed Guidance and collectively received 65 comments on the proposed Guidance. In some instances, several commenters joined in filing a single comment. The commenters included 10 bank holding companies, eight financial institution trade associations, 25 financial institutions (including three Federal Reserve Banks), five consumer groups, three payment systems, three software companies, three non-financial institution business associations, three service providers, two credit unions, a member of Congress, a state office, a compliance officer, a security and risk consultant, a trademark protection service, and a trade association representing consumer reporting agencies.

Commenters generally agreed that financial institutions should have response programs. Indeed, many financial institutions said that they have such programs in place. Comments from consumer groups and the Congressman commended the Agencies for providing guidance on response programs and customer notification. However, most industry commenters thought that the proposed Guidance was too prescriptive. These commenters stated that the proposed approach would stifle innovation and retard the effective evolution of response programs. Industry commenters raised concerns that the proposed Guidance would not permit a financial institution to assess different situations from its own business perspective, specific to its size, operational and system structure, and risk tolerances. These industry commenters suggested modifying the proposed Guidance to give financial institutions greater discretion to determine how to respond to incidents of unauthorized access to or use of customer information.

Two commenters also requested that the Agencies include a transition period allowing adequate time for financial institutions to implement the final Guidance. Some commenters asked for a transition period only for the aspects of the final Guidance that address service provider arrangements.

III. Overview of Final Guidance

The final Guidance states that every financial institution should develop and implement a response program designed to address incidents of unauthorized access to customer information maintained by the institution or its service provider. The final Guidance provides each financial institution with greater flexibility to design a risk-based response program tailored to the size, complexity and nature of its operations.

The final Guidance continues to highlight customer notice as a key feature of an institution's response program. However, in response to the comments received, the final Guidance modifies the standard describing when notice should be given and provides for a delay at the request of law enforcement. It also modifies which customers should be given notice, what a notice should contain, and how it should be delivered.

A more detailed discussion of the final Guidance and the manner in which it incorporates comments the Agencies received follows.

IV. Section-by-Section Analysis of the Comments Received

A. The "Background" Section

Legal Authority

Section I of the proposed Guidance described the legal authority for the Agencies' position that every financial institution should have a response program that includes measures to protect customer information maintained by the institution or its service providers. The proposed

Guidance also stated that the Agencies expect customer notification to be a component of the response program.

One commenter questioned the Agencies' legal authority to issue the proposed Guidance. This commenter asserted that section 501(b) only authorizes the Agencies to establish standards requiring financial institutions to safeguard the confidentiality and integrity of customer information and to protect that information from unauthorized access, but does not authorize standards that would require a response to incidents where the security of customer information actually has been breached.

The final Guidance interprets those provisions of the Security Guidelines issued under the authority of section 501(b)(3) of the GLBA, which states specifically that the standards to be established by the Agencies must include various safeguards to protect against not only "unauthorized access to," but also the "use of," customer information that could result in "substantial harm or inconvenience to any customer." This language authorizes standards that include response programs to address incidents of unauthorized access to customer information. A response program is the principal means for a financial institution to protect against unauthorized "use" of customer information that could lead to "substantial harm or inconvenience" to the institution's customer. For example, customer notification is an important tool that enables a customer to take steps to prevent identity theft, such as by arranging to have a fraud alert placed in his or her credit file. Accordingly, when evaluating the adequacy of an institution's information security program required by the Security Guidelines, the Agencies will consider whether the institution has developed and implemented a response program as described in the final Guidance.

Scope of Guidance

In a number of places throughout the proposed Guidance, the Agencies referenced definitions in the Security Guidelines. However, the Agencies did not specifically address the scope of the proposed Guidance. Commenters had questions and suggestions regarding the scope of the proposed Guidance and the meaning of terms used.

Entities and Information Covered

Some commenters had questions about the entities and information covered by the proposed Guidance. One commenter suggested that the Agencies clarify that foreign offices, branches, and affiliates of United States banks are not subject to the final Guidance. Some commenters recommended that the Agencies clarify that the final Guidance applies only to unauthorized access to sensitive information within the control of the financial institution. One commenter thought that the final Guidance should be broad and cover frauds committed against bank customers through the Internet, such as through the misuse of online corporate identities to defraud online banking customers through fake web sites (commonly known as "phishing"). Several commenters requested confirmation in the final Guidance that it applies to consumer accounts and not to business and other commercial accounts.

For greater clarity, the Agencies have revised the Background section of the final Guidance to state that the scope and definitions of terms used in the Guidance are identical to those in section 501(b) of the GLBA and the Security Guidelines which largely cross-reference definitions used in the Agencies' Privacy Rules.[5] Therefore, consistent with section 501(b) and the Security Guidelines, this final Guidance applies to the entities enumerated in section 505(a)

[5] 12 CFR part 40 (OCC); 12 CFR part 216 (Board); 12 CFR part 332 (FDIC); and 12 CFR part 573 (OTS). In this final Guidance, citations to the Agencies' Privacy Rules refer only to the appropriate section number that is common to each of these rules.

of the GLBA.[6] This final Guidance does not apply to a financial institution's foreign offices, branches, or affiliates. However, a financial institution subject to the Security Guidelines is responsible for the security of its customer information, whether the information is maintained within or outside of the United States, such as by a service provider located outside of the United States.

This final Guidance also applies to "customer information," meaning any record containing "nonpublic personal information" (as that term is defined in § __.3(n) of the Agencies' Privacy Rules) about a financial institution's customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the institution.[7] Consequently, the final Guidance applies only to information that is within the control of the institution and its service providers, and would not apply to information directly disclosed by a customer to a third party, for example, through a fraudulent web site.

Moreover, this final Guidance does not apply to information involving business or commercial accounts. Instead, the final Guidance applies to nonpublic personal information about a "customer" within the meaning of the Security Guidelines, namely, a consumer who obtains a financial product or service from a financial institution to be used primarily for

[6] National banks, Federal branches and Federal agencies of foreign banks and any subsidiaries of these entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OCC); member banks (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, Edge and Agreement Act Corporations, bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (Board); state non-member banks, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (FDIC); and insured savings associations and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OTS).

[7] See Security Guidelines, I.C.2.c.

personal, family, or household purposes, and who has a continuing relationship with the institution.[8]

Effect of Other Laws

Several commenters requested that the Agencies explain how the final Guidance interacts with additional and possibly conflicting state law requirements. Most of these commenters urged that the final Guidance expressly preempt state law. By contrast, one commenter asked the Agencies to clarify that a financial institution must also comply with additional state law requirements. In addition, some commenters asked that the final Guidance provide a safe harbor defense against class action suits. They suggested that the safe harbor should cover any financial institution that takes reasonable steps that regulators require to protect customer information, but, nonetheless, experiences an event beyond its control that leads to the disclosure of customer information.

These issues do not fall within the scope of this final Guidance. The extent to which section 501(b) of the GLBA, the Security Guidelines, and any related Agency interpretations, such as this final Guidance, preempt state law is governed by Federal law, including the procedures set forth in section 507 of GLBA, 15 U.S.C. 6807.[9] Moreover, there is nothing in Title V of the GLBA that authorizes the Agencies to provide institutions with a safe harbor defense. Therefore, the final Guidance does not address these issues.

Organizational Changes in the "Background" Section

[8] See Security Guidelines, I.C.2.b.; Privacy Rules, § __.3(h).

[9] Section 507 provides that state laws that are "inconsistent" with the provisions of Title V, Subtitle A of the GLBA are preempted "only to the extent of the inconsistency." State laws are "not inconsistent" if they offer greater protection than Subtitle A, as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under section 505(a) of either the person that initiated the complaint or that is the subject of the complaint. See 15 U.S.C. 6807.

For the reasons described earlier, the Background section is adopted essentially as proposed, except that the latter part of the paragraph on "Service Providers" and the entire paragraph on "Response Programs" are incorporated into the introductory discussion of section II. The Agencies believe that the Background section is now clearer, as it focuses solely on the statutory and regulatory framework upon which the final Guidance is based. Comments and changes with respect to the paragraphs that were relocated are discussed in the next section.

B. The "Response Program" Section

The Security Guidelines enumerate a number of security measures that each financial institution must consider and adopt, if appropriate, to control risks stemming from reasonably foreseeable internal and external threats to an institution's customer information.[10] The introductory paragraph of section II of the final Guidance specifically states that a financial institution should implement those security measures designed to prevent unauthorized access to or use of customer information, such as by placing access controls on customer information systems and conducting background checks for employees[11] who are authorized to access customer information. The introductory paragraph also states that every financial institution should develop and implement security measures designed to address incidents of unauthorized access to customer information that occur despite measures to prevent security breaches.

The measures enumerated in the Security Guidelines include "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

[10] Security Guidelines, III.B. and III.C.

[11] A footnote has been added to this section to make clear that 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).

law enforcement agencies."[12] Prompt action by both the institution and the customer following the unauthorized access to customer information is crucial to limit identity theft. As a result, every financial institution should develop and implement a response program appropriate to the size and complexity of the institution and the nature and scope of its activities, designed to address incidents of unauthorized access to customer information.

The introductory language in section II of the final Guidance states that a response program should be a key part of an institution's information security program. It also emphasizes that a financial institution's response program should be risk-based and describes the components of a response program in a less prescriptive manner.

Service Provider Contracts

The Background section of the proposed Guidance elaborated on the specific provisions that a financial institution's contracts with its service providers should contain. The proposed Guidance stated that a financial institution's contract with its service provider should require the service provider to disclose fully to the institution information related to any breach in security resulting in an unauthorized intrusion into the institution's customer information systems maintained by the service provider. It stated that this disclosure would permit an institution to expeditiously implement its response program.

Several commenters on the proposed Guidance agreed that a financial institution's contracts with its service providers should require the service provider to disclose fully to the institution information related to any breach in security resulting in an unauthorized intrusion into the institution's customer information systems maintained by the service provider. However, many commenters suggested modifications to this section.

---

[12] Security Guidelines, III.C.1.g.

The discussion of this aspect of a financial institution's contracts with its service providers is in section II of the final Guidance. It has been revised as follows in response to the comments received.

Timing of Service Provider Notification

The Agencies received a number of comments regarding the timing of a service provider's notice to a financial institution. One commenter suggested requiring service providers to report incidents of unauthorized access to financial institutions within 24 hours after discovery of the incident.

In response to comments on the timing of a service provider's notice to a financial institution, the final Guidance adds that a financial institution's contract with its service provider should require the service provider to take appropriate action to address incidents of unauthorized access to the institution's customer information, including by notifying the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program. The Agencies determined that requiring notice within 24 hours of an incident may not be practicable or appropriate in every situation, particularly where, for example, it takes a service provider time to investigate a breach in security. Therefore, the final Guidance does not specify a number of hours or days by which the service provider must give notice to the financial institution.

Existing Contracts with Service Providers

Some commenters expressed concerns that they would have to rewrite their contracts with service providers to require the disclosure described in this provision. These commenters asked the Agencies to grandfather existing contracts and to apply this provision only

prospectively to new contracts. Many commenters also suggested that the final Guidance contain a transition period to permit financial institutions to modify their existing contracts.

The Agencies have decided not to grandfather existing contracts or to add a transition period to the final Guidance because, as stated in the proposed Guidance, this disclosure provision is consistent with the obligations in the Security Guidelines that relate to service provider arrangements and with existing guidance on this topic previously issued by the Agencies.[13] In order to ensure the safeguarding of customer information, financial institutions that use service providers likely have already arranged to receive notification from the service providers when customer information is accessed in an unauthorized manner. In light of the comments received, however, the Agencies recognize that there are institutions that have not formally included such a disclosure requirement in their contracts. Where this is the case, the institution should exercise its best efforts to add a disclosure requirement to its contracts and any new contracts should include such a provision.

Thus, the final Guidance adopts the discussion on service provider arrangements largely as proposed. To eliminate any ambiguity regarding the application of this section to foreign-based service providers, however, the final Guidance now makes clear that a covered financial institution[14] should be capable of addressing incidents of unauthorized access to customer information in customer information systems maintained by its domestic and foreign service providers.[15]

---

[13] See FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, Jun. 2004; 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.

[14] See footnote 6, supra.

[15] See, e.g., FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, Jun. 2004; OCC Bulletin 2002-16 (national banks); OTS Thrift Bulletin 82a, Third Party Arrangements, Sept. 1, 2004 (savings associations).

Components of a Response Program

As described earlier, commenters criticized the prescriptive nature of proposed section II that described the four components a response program should contain. The proposed Guidance instructed institutions to design programs to respond to incidents of unauthorized access to customer information by: (1) assessing the situation; (2) notifying regulatory and law enforcement agencies; (3) containing and controlling the situation; and (4) taking corrective measures. The proposed Guidance contained detailed information about each of these four components.

The introductory discussion in this section of the final Guidance now makes clear that, as a general matter, an institution's response program should be risk-based. It applies this principle by modifying the discussion of a number of these components. The Agencies determined that the detailed instructions in these components of the proposed Guidance, especially in the "Corrective Measures" section, would not always be relevant or appropriate. Therefore, the final Guidance describes, through brief bulleted points, the elements of a response program, giving financial institutions greater discretion to address incidents of unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

At a minimum, an institution's response program should contain procedures for: (1) assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused; (2) 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 later in the final Guidance; (3) immediately notifying law enforcement in situations involving Federal criminal violations requiring immediate attention; (4) taking appropriate steps to contain and

control the incident to prevent further unauthorized access to or use of customer information, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and (5) notifying customers when warranted.

Assess the Situation

The proposed Guidance stated that an 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.

Some commenters stated that the Agencies should retain this provision in the final Guidance. One commenter suggested that an institution should focus its entire response program primarily on addressing unauthorized access to sensitive customer information.

The Agencies have concluded that a financial institution's response program should begin with a risk assessment that allows an institution to establish the nature of any information improperly accessed. This will allow the institution to determine whether and how to respond to an incident. Accordingly, the Agencies have not changed this provision.

Notify Regulatory and Law Enforcement Agencies

The proposed Guidance provided that an 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 customers. In addition, the proposed Guidance stated that an institution should file a Suspicious Activity Report (SAR), if required, in accordance with the applicable SAR regulations[16] and various

[16] 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).

Agency issuances.[17] The proposed Guidance stated that, consistent with the Agencies' SAR regulations, in situations involving Federal criminal violations requiring immediate attention, the institution immediately should notify, by telephone, the appropriate law enforcement authorities and its primary regulator, in addition to filing a timely SAR. For the sake of clarity, the final Guidance discusses notice to regulators and notice to law enforcement in two separate bulleted items.

Standard for Notice to Regulators

The provision regarding notice to regulators in the proposed Guidance prompted numerous comments. Many commenters suggested that the Agencies adopt a narrow standard for notifying regulators. These commenters were concerned that notice to regulators, provided under the circumstances described in the proposed Guidance, would be unduly burdensome for institutions, service providers, and regulators, alike.

Some of these commenters suggested that the Agencies adopt the same standard for notifying regulators and customers. These commenters recommended that notification occur when an institution becomes aware of an incident involving unauthorized access to or use of "sensitive customer information," a defined term in the proposed Guidance that specified a subset of customer information deemed by the Agencies as most likely to be misused.

Other commenters recommended that the Agencies narrow this provision so that a financial institution would inform a regulator only in connection with an incident that poses a

[17] 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); OCC AL 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 OCC AL 2001-4, Identity Theft and Pretext Calling, April 30, 2001; 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; http://www.ots.treas.gov/BSA (for the latest SAR form and filing instructions required by OTS as of July 1, 2003).

significant risk of substantial harm to a significant number of its customers, or only in a situation where substantial harm to customers has occurred or is likely to occur, instead of when it could occur.

Other commenters who advocated the adoption of a narrower standard asked the Agencies to take the position that filing a SAR constitutes sufficient notice and that notification of other regulatory and law enforcement agencies is at the sole discretion of the institution. One commenter stated that it is difficult to imagine any scenario that would trigger the response program without requiring a SAR filing. Some commenters asserted that if the Agencies believe a lower threshold is advisable for security breaches, the Agencies should amend the SAR regulations.

By contrast, some commenters recommended that the standard for notification of regulators remain broad. One commenter advocated that any event that triggers an internal investigation by the institution should require notice to the appropriate regulator. Another commenter similarly suggested that notification of all security events to federal regulators is critical, not only those involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers.

The Agencies have concluded that the standard for notification to regulators should provide an early warning to allow an institution's regulator to assess the effectiveness of an institution's response plan, and, where appropriate, to direct that notice be given to customers if the institution has not already done so. Thus, the standard in the final Guidance states that an institution should notify 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."

"Sensitive customer information" is defined in section III of the final Guidance and 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.

This standard is narrower than that in the proposed Guidance because a financial institution will need to notify its regulator only if it becomes aware of an incident involving "sensitive customer information." Therefore, under the final Guidance, there will be fewer occasions when a financial institution should need to notify its regulators. However, under this standard, a financial institution will need to notify its regulator at the time that the institution initiates its investigation to determine the likelihood that the information has been or will be misused, so that the regulator will be able to take appropriate action, if necessary.

Method of Providing Notice to Regulators

Commenters on the proposed Guidance also questioned how a financial institution should provide notice to its regulator. One commenter suggested that the Agencies should standardize the notice that financial institutions provide to their regulators. The commenter suggested that the Agencies use these notices to track institutions' compliance with the Security Guidelines, gather comprehensive details regarding each incident, and track other statistical data regarding security. The statistical data could include the number of security incidents reported annually and the number of times the incidents warranted customer notice.

The Agencies do not wish to create another SAR-like process that requires the completion of detailed forms. Instead, the Agencies contemplate that a financial institution will notify regulators as quickly as possible, by telephone, or in some other expeditious manner when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. The Agencies believe that the extent to which they will gather statistics on security incidents and customer notice is beyond the scope of the final Guidance. Whether or not an Agency will track the number of incidents reported is left to the discretion of individual Agencies.

Notice to Regulators by Service Providers

Commenters on the proposed Guidance questioned whether a financial institution or its service provider should give notice to a regulator when a security incident involves an unauthorized intrusion into the institution's customer information systems maintained by the service provider. One commenter noted that if a security event occurs at a large service provider, regulators could receive thousands of notices from institutions relating to the same event. The commenter suggested that if a service provider is examined by one of the Agencies the most efficient means of providing regulatory notice of such a security event would be to allow the servicer to notify its primary Agency contact. The primary Agency contact then could disseminate the information to the other regulatory agencies as appropriate.

The Agencies believe that it is the responsibility of the financial institution and not the service provider to notify the institution's regulator. Therefore, the final Guidance states that a financial institution should notify 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. Nonetheless, a security incident at a service provider could have an

impact on multiple financial institutions that are supervised by different Federal regulators. Therefore, in the interest of efficiency and burden reduction, the last paragraph in section II of the final Guidance makes clear that an institution may authorize or contract with its service provider to notify the institution's regulator on the institution's behalf when a security incident involves an unauthorized intrusion into the institution's customer information systems maintained by the service provider.

Notice to Law Enforcement

Some commenters took issue with the provision in the proposed Guidance regarding notification of law enforcement by telephone. One commenter asked the Agencies to clarify how notification of law enforcement by telephone would work since in many cases it is unclear what telephone number should be used. This commenter maintained that size and sophistication of law enforcement authorities may differ from state to state and this requirement may create confusion and unwarranted action by the law enforcement authority.

The final Guidance adopts this provision as proposed. The Agencies note that the provision stating that an institution should notify law enforcement by telephone in situations involving Federal criminal violations requiring immediate attention is consistent with the Agencies' existing SAR regulations.[18]

Contain and Control the Situation

The proposed Guidance stated that the financial institution should take measures to contain and control a security incident to prevent further unauthorized access to or use of customer information while preserving records and other evidence.[19] It also stated that,

---

[18] See footnote 16, supra.

[19] See FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002, pp. 68-74 available at: http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm.

depending upon the particular facts and circumstances of the incident, measures in connection with computer intrusions could include: (1) shutting down applications or third party connections; (2) reconfiguring firewalls in cases of unauthorized electronic intrusion; (3) ensuring that all known vulnerabilities in the financial institution's computer systems have been addressed; (4) changing computer access codes; (5) modifying physical access controls; and (6) placing additional controls on service provider arrangements.

Few comments were received on this section. One commenter suggested that the Agencies adopt this section unchanged in the final Guidance. Another commenter had questions about the meaning of the phrase "known vulnerabilities." Commenters did, however, note the overlap between proposed section II.C., and the corrective measures in proposed section II.D., described as "flagging accounts" and "securing accounts."

The Agencies agree that some sections in the proposed Guidance overlapped. Therefore, the Agencies modified this section by incorporating concepts from the proposed Corrective Measures component, and removing the more specific examples in this section, including the terms that confused commenters. This section in the final Guidance gives an institution greater discretion to determine the measures it will take to contain and control a security incident. It states that institutions should take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence.

Preserving Evidence

One commenter stated that the final Guidance should require financial institutions, as part of the response process, to have an effective computer forensics capability in order to investigate and mitigate computer security incidents as discussed in principle fourteen of the Basel

Committee's "Risk Management for Electronic Banking"[20] and the International Organization for Standardization's ISO 17799.[21]

The Agencies note that the final Guidance addresses not only computer security incidents, but also all other incidents of unauthorized access to customer information. Thus, it is not appropriate to include more detail about steps an institution should take to investigate and mitigate computer security incidents. However, the Agencies believe that institutions should be mindful of industry standards when investigating an incident. Therefore, the final Guidance contains a reference to forensics by generally noting that an institution should take appropriate steps to contain and control an incident, while preserving records and other evidence.

Corrective Measures

The proposed Guidance stated that once a financial 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. It then described three corrective measures that a financial institution should include as a part of its response program in order to effectively address and mitigate harm to individual customers: (1) flagging accounts; (2) securing accounts; and (3) notifying customers. The Agencies removed the first two corrective measures for the reasons that follow.

Flagging and Securing Accounts

The first corrective measure in the proposed Guidance directed financial institutions to "flag accounts." It stated that an institution should immediately begin identifying and monitoring the accounts of those customers whose information may have been accessed or misused. It also stated that an institution should provide staff with instructions regarding the

[20] http://www.bis.org/publ/bcbs35.htm.
[21] http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.

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.

The second corrective measure directed institutions to "secure accounts." The proposed Guidance stated that 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 services that can be accessed using the same account number or name and password combination. The proposed Guidance stated that accounts should be secured until such time as the financial institution and the customer agree on a course of action.

Commenters were critical of these proposed measures. Several commenters asserted that the final Guidance should not prescribe responses to security incidents with this level of detail. Other commenters recommended that if the Agencies chose to retain references to "flagging" or "securing" accounts, they should include the words "where appropriate" in order to give institutions the flexibility to choose the most effective solutions to problems.

Commenters also stated that the decision to flag accounts, the nature of that flag, and the duration of the flag, should be left to an individual financial institution's risk-based procedures developed under the Security Guidelines. These commenters asked the Agencies to recognize that regular, ongoing fraud prevention and detection methods employed by an institution may be sufficient.

Commenters representing small institutions stated that they do not have the technology or other resources to monitor individual accounts. They stated that the financial impact of having to monitor accounts for unusual activity would be enormous, as each institution would have to

purchase expensive technology, hire more personnel, or both. These commenters asked the Agencies to provide institutions with the flexibility to close an account if the institution detects unusual activity.

With respect to "securing accounts," several commenters stated that if "secure" means close or freeze, either action would be extreme and would have significant adverse consequences for customers. Other commenters stated that the requirement that the institution and the customer "agree on a course of action" is unrealistic, unworkable and should be eliminated. Some commenters explained that if a customer is traveling and the financial institution cannot contact the customer to obtain the customer's consent, freezing or closing a customer's account could strand the customer with no means of taking care of expenses. They stated that, in the typical case, the institution would monitor such an account for suspicious transactions.

As described earlier, the Agencies are adopting an approach in the final Guidance that is more flexible and risk-based than that in the proposed Guidance. The final Guidance incorporates the general concepts described in the first two corrective measures into the brief bullets describing components of a response program enumerated in section II.C. Therefore, the first and second corrective measures no longer appear in the final Guidance.

Customer Notice and Assistance

The third corrective measure in the proposed Guidance was titled "Customer Notice and Assistance." This proposed measure stated that a financial institution should notify and offer assistance to customers whose information was the subject of an incident of unauthorized access or use under the circumstances described in section III of the proposed Guidance. The proposed Guidance also described which customers should be notified. In addition, this corrective measure contained provisions discussing delivery and contents of the customer notice.

The final Guidance now states that an institution's response program should contain procedures for notifying customers when warranted. For clarity's sake, the discussion of which customers should be notified, and the delivery and contents of customer notice, is now in new section III, titled "Customer Notice." Comments and changes with respect to the paragraphs that were relocated are discussed under the section titled "Customer Notice" that follows.

Responsibility for Notice to Customers

Some commenters were confused by the discussion in the proposed Guidance stating that a financial institution's contract with its service provider should require the service provider to disclose fully to the institution information related to any breach in security resulting in an unauthorized intrusion into the institution's customer information systems maintained by the service provider. Commenters stated that this provision appears to create an obligation for both financial institutions and their service providers to provide notice of security incidents to the institution's customers. These commenters recommended that the service provider notify its financial institution customer so that the financial institution could provide appropriate notice to its customers. Thus, customers would avoid receiving multiple notices relating to a single security incident.

Other commenters asserted that a financial institution should not have to notify its customers if an incident has occurred because of the negligence of its service provider. These commenters recommended that in this situation, the service provider should be responsible for providing notice to the financial institution's customers.

As discussed above in connection with notice to regulators, the Agencies believe that it is the responsibility of the institution, and not of the service provider, to notify the institution's customers in connection with an unauthorized intrusion into an institution's customer

information systems maintained by the service provider. The responsibility to notify customers remains with the institution whether the incident is inadvertent or due to the service provider's negligence. The Agencies note that the costs of providing notice to the institution's customers as a result of negligence on the part of the service provider may be addressed in the financial institution's contract with its service provider.

The last paragraph in section II of the final Guidance, therefore, states that it is the responsibility of the financial institution to notify the institution's customers. It also states that the institution may authorize or contract with its service provider to notify customers on the institution's behalf, when a security incident involves an unauthorized intrusion into the institution's customer information systems maintained by the service provider.

C. The "Customer Notice" Section

Section III of the proposed Guidance described the standard for providing notice to customers and defined the term "sensitive customer information" used in that standard. This section also gave examples of circumstances when a financial institution should give notice and when the Agencies do not expect a financial institution to give notice. It also discussed contents of the notice and proper delivery.

Section III of the final Guidance similarly describes the standard for providing notice to customers and defines both the terms "sensitive customer information" and "affected customers." It also discusses the contents of the notice and proper delivery.

Standard for Providing Notice

A key feature of the proposed Guidance was the description of when a financial institution should provide customer notice. The proposed Guidance stated that 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.

The Agencies believed that this proposed standard would strike a balance between notification to customers every time the mere possibility of misuse of customer information arises from unauthorized access and a situation where the financial institution knows with certainty that information is being misused. However, the Agencies specifically requested comment on whether this is the appropriate standard and invited commenters to offer alternative thresholds for customer notification.

Some commenters stated that the proposed standard was reasonable and sufficiently flexible. However, many commenters recommended that the Agencies provide financial institutions with greater discretion to determine when a financial institution should notify its customers. Some of these commenters asserted that a financial institution should not have to give notice unless the institution believes it "to be reasonably likely," or if circumstances indicated "a significant risk" that the information will be misused.

Commenters maintained that because the proposed standard states that a financial institution should give notice when fraud or identity theft is merely possible, notification under these circumstances would needlessly alarm customers where little likelihood of harm exists. Commenters claimed that, eventually, frequent notices in non-threatening situations would be perceived by customers as routine and commonplace, and therefore reduce their effectiveness.

The Agencies believe that articulating as part of the guidance a standard that sets forth when notice to customers is warranted is both helpful and appropriate. However, the Agencies

agree with commenters and are concerned that the proposed threshold inappropriately required institutions to prove a negative proposition, namely, that misuse of the information accessed is unlikely to occur. In addition, the Agencies do not want customers of financial institutions to receive notices that would not be useful to them. Therefore, the Agencies have revised the standard for customer notification.

The final Guidance provides that when an institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused. If the institution determines that misuse of the information has occurred or is reasonably possible, it should notify affected customers as soon as possible.

An investigation is an integral part of the standard in the final Guidance. A financial institution should not forego conducting an investigation to avoid reaching a conclusion regarding the likelihood that customer information has been or will be misused and cannot unreasonably limit the scope of the investigation. However, the Agencies acknowledge that a full-scale investigation may not be necessary in all cases, such as where the facts readily indicate that information will or will not be misused.

Monitoring for Suspicious Activity

The proposed Guidance stated that an institution need not notify customers if it 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. A number of comments addressed the standard in the proposed Guidance on monitoring affected customers' accounts for unusual or suspicious activity.

Some commenters stated that the final Guidance should grant institutions the discretion to monitor the affected customer accounts for a period of time and to the extent warranted by the particular circumstances. Some commenters suggested that monitoring occur during the investigation. One commenter noted that an institution's investigation may reveal that monitoring is unnecessary. One commenter noted that monitoring the customer's accounts at the institution may not protect the customer, because unauthorized access to customer information may result in identity theft beyond the accounts held at the specific financial institution.

The Agencies agree that under certain circumstances, monitoring may be unnecessary, for example when, on the basis of a reasonable investigation, an institution determines that information was not misused. The Agencies also agree that the monitoring requirement may not protect the customer. Indeed, an identity thief with unauthorized access to certain sensitive customer information likely will open accounts at other financial institutions in the customer's name. Accordingly, the Agencies conclude that monitoring under the circumstances described in the standard for notice would be burdensome for financial institutions without a commensurate benefit to customers. For these reasons, the Agencies have removed the reference to monitoring in the final Guidance.

Timing of Notice

The proposed Guidance did not include specific language on the timing of notice to customers and the Agencies received many comments on this issue. Some commenters requested clarification of the time frame for customer notice. One commenter recommended that the Agencies adopt the approach in the proposed Guidance because it did not set forth any circumstances that may delay notification of the affected customers. Yet another commenter maintained that, in light of a customer's need to act expeditiously against identity theft, an

outside limit of 48 hours after the financial institution learns of the breach is a reasonable and timely requirement for notice to customers. Many commenters, however, recommended that the Agencies make clear that an institution may take the time it reasonably needs to conduct an investigation to assess the risk resulting from a security incident.

The Agencies have responded to these various comments on the timing of notice by providing that a financial institution notify an affected customer "as soon as possible" after concluding that misuse of the customer's information has occurred or is reasonably possible. As the scope and timing of a financial institution's investigation is dictated by the facts and circumstances of a particular case, the Agencies have not designated a specific number of hours or days by which financial institutions should provide notice to customers. The Agencies believe that doing so may inhibit an institution's ability to investigate adequately a particular incident or may result in notice that is not timely.

Delay for Law Enforcement Investigation

The proposed Guidance did not address delay of notice to customers while a law enforcement investigation is conducted. Many commenters recommended permitting an institution to delay notification to customers to avoid compromising a law enforcement investigation. These commenters noted that the California Database Protection Act of 2003 (CDPA) requires notification of California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[22] However, the CDPA permits a delay in notification if a law enforcement agency determines that the notification will impede a criminal investigation.[23] Another commenter suggested that an

[22] See CAL. CIV. CODE § 1798.82 (West 2005).
[23] See CAL. CIV. CODE § 1798.82(c) (West 2005).

institution should not have to obtain a formal determination from a law enforcement agency before it is able to delay notice.

The Agencies agree that it is appropriate to delay customer notice if such notice will jeopardize a law enforcement investigation. However, to ensure that such a delay is necessary and justifiable, the final Guidance states that 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. [24]

The Agencies are concerned that a delay of notification for a law enforcement investigation could interfere with the ability of customers to protect themselves from identity theft and other misuse of their sensitive information. Thus, the final Guidance also provides that a financial institution should notify its customers as soon as notification will no longer interfere with the investigation and should maintain contact with the law enforcement agency that has requested a delay, in order to learn, in a timely manner, when customer notice will no longer interfere with the investigation.

Sensitive Customer Information

Scope of Standard

The Agencies received many comments on the limitation of notice in the proposed Guidance to incidents involving unauthorized access to sensitive customer information. The Agencies invited comment on whether to modify the proposed standard for notice to apply to other 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.

[24] This includes circumstances when an institution confirms that an oral request for delay from law enforcement will be followed by a written request.

Most commenters recommended that the standard remain as proposed rather than covering other types of information. One commenter suggested that the Agencies continue to allow a financial institution the discretion to notify affected customers in any other extraordinary circumstances that compel it to conclude that unauthorized access to information other than sensitive customer information likely will result in substantial harm or inconvenience to those affected. However, the commenter did not provide any examples of such extraordinary circumstances.

The Agencies continue to believe that the rationale for limiting the standard to sensitive customer information expressed in the proposed Guidance is correct. The proposed Guidance explained that, 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 a 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.

The Agencies have not identified any other circumstances that should prompt customer notice and continue to believe that it is not likely that a customer will suffer substantial harm or inconvenience from unauthorized access to other types of information. Therefore, the standard in the final Guidance continues to be limited to unauthorized access to sensitive customer information. Of course, a financial institution still may send notices to customers in any additional circumstances that it determines are appropriate.

Definition of Sensitive Customer Information

The Agencies received many comments on the proposed definition of "sensitive customer information" in the proposed Guidance. The first part of the proposed definition stated that

"sensitive customer information" is a customer's social security number, personal identification number (PIN), password or account number, in conjunction with a personal identifier such as the customer's name, address, or telephone number. In addition, the second part of the proposed definition stated that "sensitive customer information" includes any combination of components of customer information that allow someone to log onto or access another person's account, such as user name and password.

Some commenters agreed with this definition of "sensitive customer information." They said that it was sound, workable, and sufficiently detailed. However, many commenters proposed additions, exclusions, or alternative definitions.

Additional Elements

Some commenters suggested that the Agencies add various data elements to the definition of sensitive customer information, including a driver's license number or number of other government-issued identification, mother's maiden name, and date of birth. One commenter suggested inclusion of other information that institutions maintain in their customer information systems such as a customer's account balance, account activity, purchase history, and investment information. The commenter noted that misuse of this information in combination with a personal identifier can just as easily result in substantial harm or inconvenience to a customer.

The Agencies have added to the first part of the definition several more specific components, such as driver's license number and debit and credit card numbers, because this information is commonly sought by identity thieves. However, the Agencies determined that the second part of the definition would cover the remaining suggestions. For example, where date of birth or mother's maiden name are used as passwords, under the final Guidance they will be

considered components of customer information that allow someone to log onto or access another person's account. Therefore, these specific elements have not been added to the definition.

Exclusions

Commenters also asserted that the proposed definition of sensitive customer information was too broad and proposed various exclusions. For example, some commenters asked the Agencies to exclude publicly available information, and also suggested that the final Guidance apply only to account numbers for transaction accounts or other accounts from which withdrawals or transfers can be initiated. These commenters explained that access to a mortgage account number (which may also be a public record) does not permit withdrawal of additional funds or otherwise damage the customer. Other commenters requested that the Agencies exclude encrypted information. Some of these commenters noted that only unencrypted information is covered by the CDPA.[25]

The final Guidance does not adopt any of the proposed exclusions. The Agencies believe it would be inappropriate to exclude publicly available information from the definition of sensitive customer information, where publicly available information is otherwise covered by the definition of "customer information."[26] So for instance, while a personal identifier, i.e., name, address, or phone number, may be publicly available, it is sensitive customer information when linked with particular nonpublic information such as a credit card account number. However, where the definition of "customer information" does not cover publicly available information, sensitive customer information also would not cover publicly available information. For instance, where an individual's name or address is linked with a mortgage loan account number

[25] See CAL. CIV. CODE § 1798.82(a) (West 2005).
[26] See Security Guidelines, I.C.2.c.

that is in the public record and, therefore, would not be considered "customer information,"[27] it also would not be considered "sensitive customer information" for purposes of the final Guidance.

In addition, access to a customer's personal information and account number, regardless of whether it is an account from which withdrawals or transfers can be initiated, may permit an identity thief to access other accounts from which withdrawals can be made. Thus, the Agencies have determined that the definition of account number should not be limited as suggested by commenters. The Agencies also believe that a blanket exclusion for all encrypted information is not appropriate, because there are many levels of encryption, some of which do not effectively protect customer information.

Alternative Definitions

Most alternative definitions suggested by commenters resembled the definition of "personal information" under the CDPA.[28] Under the CDPA, "personal information" includes a resident of California's name together with an account number, or credit or debit card number only if the information accessed also includes any required security code, access code, or password that would permit access to an individual's financial account. Therefore, some commenters asked that the final Guidance clarify that a name and an account number, together, is not sensitive customer information unless these elements are combined with other information that permits access to a customer's financial account.

---

[27] See § __.3(p)(3)(i).

[28] Under California law requiring notice, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) social security number; (2) driver's license number or California Identification Card number; (3) account number, credit or debit card number, in combination with any required security code access code, or password that would permit access to an individual's financial account. See CAL. CIV. CODE § 1798.82(e) (West 2005).

The Agencies concluded that it would be helpful if financial institutions could more easily compare and contrast the definition of "personal information" under the CDPA with the definition of "sensitive information" under the Final Guidance. Therefore, the elements in the definition of sensitive information in the final Guidance are re-ordered and the Agencies added the elements discussed earlier.

The final Guidance states that 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. The final Guidance also states that sensitive customer information 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 a password and account number.

The Agencies decline to adopt the CDPA standard for several reasons. First, for example, under the CDPA, personal information includes a person's name in combination with other data elements. By contrast, the final Guidance treats address and telephone number in the same manner as a customer's name, because reverse directories may permit an address or telephone number to be traced back to an individual customer.

In addition, under the CDPA, "personal information" includes name together with an account number, or credit or debit card number only if the information accessed also includes any required security code, access code, or password that would permit access to an individual's financial account. The Agencies note that a name and account number, alone, is sufficient to create fraudulent checks, or to direct the unauthorized debit of a customer's account even

without an access code.[29] Further, a name and credit card number may permit unauthorized access to a customer's account. Therefore, the final Guidance continues to define a customer's name and account number, or credit or debit card number as sensitive customer information.

Affected Customers

The Agencies received many comments on the discussion of notice to "affected customers" in the proposed Guidance. Section II.D.3. of the proposed Guidance provided that if the institution could determine from its logs or other data precisely which customers' information was accessed or misused, it could restrict its notification to those individuals. However, if the institution could not identify precisely which customers were affected, it should notify each customer in any group likely to have been affected, such as each customer whose information was stored in the group of files in question.

Commenters were concerned that this provision in the proposed Guidance was overly broad. These commenters stated that providing notice to all customers in groups likely to be affected would result in many notices that are not helpful. The commenters suggested that the final Guidance narrow the standard for notifying customers to only those customers whose information has been or is likely to be misused.

The discussion of "affected customers" has been relocated and is separately set forth following the definition of "sensitive customer information," in the final Guidance. The discussion of "affected customers" in the final Guidance states that if a financial institution, based upon its investigation, can determine from its logs or other data precisely which

[29] See, e.g., Griff Witte, Bogus Charges, Unknowingly Paid: FTC Accuses 2 of Raiding 90,000 Bank Accounts in Card Fraud,, Washington Post, May 29, 2004, at E1 (list of names with associated checking account numbers used by bogus company to debit bank accounts without customer authorization).

customers' information has been improperly accessed,[30] it may notify only those customers with respect to whom the institution determines that misuse of their information has occurred or is reasonably possible. However, the final Guidance further notes that 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 contained in the group of files is reasonably possible, it should notify all customers in the group. In this way, the Agencies have reduced the number of notices that should be sent.

Examples

The proposed Guidance described several examples of when a financial institution should give notice and when the Agencies do not expect a financial institution to give notice.

The Agencies received a number of comments on the examples. Some commenters thought the examples were helpful and suggested that the Agencies add more. Other commenters criticized the examples as too broad. Many commenters suggested numerous ways to modify and clarify the examples.

Since the examples in the proposed Guidance led to interpretive questions, rather than interpretive clarity, the Agencies concluded that it is not particularly helpful to offer examples of when notice is and is not expected. In addition, the Agencies believe that the standard for notice itself has been clarified and examples are no longer necessary. Therefore, there are no examples in the final Guidance.

[30] The Agencies note that system logs may permit an institution to determine precisely which customers' data has been improperly accessed. See, e.g., FFIEC Information Technology Handbook, Information Security Booklet, page 64 available at http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm.

Content of Customer Notice

The Agencies received many comments on the discussion of the content of customer notice located in section II.D.3.b. of the proposed Guidance. The proposed Guidance stated that a notice should describe the incident in general terms and the customer's information that was the subject of unauthorized access or use. It stated that the notice should also include a number that customers can call for further information and assistance, remind customers of the need to remain vigilant over the next 12 to 24 months, and recommend that customers promptly report incidents of suspected identity theft. The proposed Guidance described several "key elements" that a notice should contain. It also provided a number of "optional elements" namely, examples of additional assistance that institutions have offered.

Some commenters agreed that the proposed Guidance sufficiently addressed most of the key elements necessary for an effective notice. However, many commenters requested greater discretion to determine the content of the notices that financial institutions provide to customers. Commenters suggested that the Agencies make clear that the various items suggested for inclusion in any customer notice are suggestions, and that not every item is mandatory in every notice.

Some commenters took issue with the enumerated items in the proposed Guidance identified as key elements that a notice should contain. For example, many commenters asserted that customers should not necessarily be encouraged to place fraud alerts with credit bureaus in every circumstance. Some of these commenters noted that not all situations will warrant having a fraud alert posted to the customer's credit file, especially if the financial institution took appropriate action to render the information accessed worthless. According to these commenters, the consequences of a fraud alert, such as increased obstacles to obtaining credit,

may outweigh any benefit. Some commenters also noted that a proliferation of fraud alerts not related to actual fraud would dilute the effectiveness of the alerts.

Other commenters criticized the optional elements in the proposed Guidance. For instance, some commenters stated that a notice should not inform the customer about subscription services that provide notification to the customer when 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. These commenters asserted that customer notices should not be converted into a marketing opportunity for subscription services provided by consumer credit bureaus. They stated that offering the service could mislead the customer into believing that these expensive services are essential. If the service is offered free of charge, an institution's choice of service could be interpreted as an endorsement for a specific company and its product.

As a result of the Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1985-86 (the FACT Act), many of the descriptions of "key elements" and "optional elements" in the proposed Guidance, and comments on these elements, have been superceded. For example, the frequency and circumstances under which a customer may obtain a credit report free-of-charge have changed.

The final Guidance continues to specify that a notice should describe the incident in general terms and the customer's information that was the subject of unauthorized access or use. It also continues to state that the notice should include a number that customers can call for further information and assistance, remind customers of the need to remain vigilant over the next 12 to 24 months, and recommend that customers promptly report incidents of suspected identity theft. In addition, the final Guidance also states that the notice should generally describe what the institution has done to protect the customers' information from further unauthorized access.

However, the final Guidance no longer distinguishes between certain other "key" items that the notice should contain and those that are "optional." The Agencies added greater flexibility to this section to accommodate any new protections afforded to consumers that flow from the FACT Act. Instead of distinguishing between items that the notice should contain and those that are optional, an institution may now select those items that are appropriate under the circumstances, and that are compatible with the FACT Act. Of course, institutions may incorporate additional information that is not mentioned in the final Guidance, where appropriate.

Coordination with Credit Reporting Agencies

A trade association representing credit reporting agencies commented that its members are extremely concerned about their ability to comply with all of the duties (triggered under the FACT Act) that result from notices financial institutions send to their customers. This commenter strongly recommended that until a financial institution has contacted each nationwide consumer reporting agency to coordinate the timing, content, and staging of notices as well as the placement of fraud alerts, as necessary, a financial institution should refrain from issuing notices suggesting that customers contact nationwide consumer reporting agencies.

The commenter also stated that a financial institution that includes such suggestions in a notice to its customers should work with the credit reporting agencies to purchase the services the financial institution believes are necessary to protect its customers. The commenter stated that the costs of serving the millions of consumers it projects would receive notices under the proposed Guidance cannot be borne by the nationwide consumer reporting agencies.

The commenter also noted that the State of California has provided clear guidance in connection with its law requiring notice and also suggested that coordination with consumer

reporting agencies is vital to ensure that a consumer can in fact request a file disclosure in a timely manner. This commenter stated that similar guidance at the federal level is essential.

The Agencies believe that the final Guidance addresses this commenter's concerns in several ways. First, for the reasons described earlier, the standard for customer notice in the final Guidance likely will result in financial institutions sending fewer notices than under the proposed Guidance. Second, the final Guidance does not require financial institutions to send notices suggesting that consumers contact the nationwide credit reporting agencies, in every case. Institutions can use their discretion to determine whether such information should be included in a notice.

It is clear, however, that customer notice may prompt more consumer contacts with credit reporting agencies, as predicted by the commenter. Therefore, the final Guidance encourages a financial institution that includes in its notice contact information for nationwide consumer reporting agencies to notify the consumer reporting agencies in advance, prior to sending large numbers of such notices. In this way, the reporting agencies will be on notice that they may have to accommodate additional requests for the placement of fraud alerts, where necessary.

Model Notice

Some commenters stated that if mandatory elements are included in the final Guidance, the Agencies should develop a model notice that incorporates all the mandated elements yet allows financial institutions to incorporate additional information where appropriate.

Given the flexibility that financial institutions now have to craft a notice tailored to the circumstances of a particular incident, the Agencies believe that any single model notice will be of little use. Therefore, the final Guidance does not contain a model notice.

Other Changes Regarding the Content of a Notice

The general discussion of the content of a notice in the final Guidance states that financial institutions should give the customer notice in a "clear and conspicuous manner." In addition, the final Guidance adopts a commenter's suggestion that financial institutions should generally describe what the institution has done to protect a customer's information from further unauthorized access so that a customer can make decisions regarding the institution's customer service. This addition allows a customer to take measures to protect his or her accounts that are not redundant or in conflict with the institution's actions.

The final Guidance also states that notice should include a telephone number that customers can call for further information and assistance. The Agencies added a new footnote to this text, which explains that the institution should ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

Delivery of Customer Notice

The Agencies received numerous suggestions regarding the delivery of customer notice located in section II.D.3.a. of the proposed Guidance. The proposed Guidance stated that customer notice should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the customer is likely to receive it. The proposed Guidance provided several examples of proper delivery and stated that an institution may choose to contact all customers affected by telephone or by mail, or for those customers who conduct transactions electronically, using electronic notice.

One commenter representing a large bank trade association agreed that this was a correct standard. However, many other commenters recommended that if it costs an institution more than $250,000 to provide notice to customers, if the affected class of persons to be notified

exceeds 500,000, or if an incident warrants large distributions of notices, the final Guidance should permit various forms of mass distribution of information, such as by postings on an Internet web page and in national or regional media outlets. Commenters explained that the CDPA contains such a provision.[31]

One commenter suggested that a financial institution should only provide notice in response to inquiries. By contrast, other commenters stated that the final Guidance should make clear that general notice on a web site is inadequate and that financial institutions should provide individual notice to customers.

The Agencies determined that the provision in the proposed Guidance that notice be delivered in a "timely, clear, and conspicuous" manner already appears elsewhere in the Guidance and does not relate to manner of delivery. This phrase appears elsewhere in the final Guidance and is unnecessary here.

The Agencies have decided not to include a provision in the final Guidance that permits notice through a posting on the web or through the media in order to provide notice to a specific number of customers or where the cost of notice to individual customers would exceed a specific dollar amount. The Agencies believe that the thresholds suggested by commenters would not be appropriate in every case, especially in connection with incidents involving smaller institutions.

Therefore, the final Guidance states that customer notice should be delivered in any manner that is designed to ensure that a customer can reasonably be expected to receive it. This standard places the responsibility on the financial institution to select a method to deliver notice that is designed to ensure that a customer is likely to receive notice.

The final Guidance also provides examples of proper delivery noting that an institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for

---

[31] See CAL. CIV. CODE § 1798.82(g)(3) (West 2005).

those customers for whom it has a valid e-mail address and who have agreed to receive electronic communications from the institution.

Some commenters questioned the effect of other laws on the proposed Guidance. A few commenters noted that electronic notice should conform to the requirements of the Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C. 7001 et seq.

The final Guidance does not discuss a financial institution's obligations under the E-Sign Act. The Agencies note that the final Guidance specifically contemplates that a financial institution may give notice electronically or by telephone. There is no requirement that notice be provided in writing. Therefore, the final Guidance does not trigger any consent requirements under the E-Sign Act.[32]

Still other commenters requested clarification that a telephone call made to a customer for purposes of complying with the final Guidance is for "emergency purposes" under the Telephone Consumer Protection Act, 47 U.S.C. 227 (TCPA). These commenters noted that this is important because under the TCPA and its implementing regulation,[33] it is unlawful to initiate a telephone call to any residential phone line using an artificial or prerecorded voice to deliver a message, without the prior express consent of the called party, unless such call is for "emergency purposes."

The final Guidance does not address the TCPA, because the TCPA is interpreted by the Federal Communications Commission (FCC), and the FCC has not yet taken a position on this issue.[34]

---

[32] Under the E-Sign Act, if a statute, regulation, or other rule of law requires that information be provided or made available to a consumer in writing, certain consent procedures apply. See 15 U.S.C. 7001(c).

[33] 47 CFR 64.1200.

[34] The Agencies note, however, that the TCPA and its implementing regulations generally exempt calls made to any person with whom the caller has an established business relationship at the time the call is made. See, e.g., 47 CFR 64.1200(a)(1)(iv). Thus, the TCPA would not appear to prohibit a financial institution's telephone calls to its own customers. In addition, the FCC's regulations state that the phrase for "emergency purposes" means calls made

V. Effective Date

Many commenters noted that the proposed Guidance did not contain a delayed effective date. They suggested that the Agencies include a transition period to allow adequate time for financial institutions to implement the final Guidance.

The final Guidance is an interpretation of existing provisions in section 501(b) of the GLBA and the Security Guidelines. A delayed effective date is not required under the APA, 12 U.S.C. 553(d)(2), or the Riegle Community Development and Regulatory Improvement Act of 1994, 12 U.S.C. 4802, which requires a delayed effective date for new regulations, because the final Guidance is a statement of policy.

Given the comments received, the Agencies recognize that not every financial institution currently has a response program that is consistent with the final Guidance. The Agencies expect these institutions to implement the final Guidance as soon as possible. However, we appreciate that some institutions may need additional time to develop new compliance procedures, modify systems, and train staff in order to implement an adequate response program. The Agencies will take into account the good faith efforts made by each institution to develop a response program that is consistent with the final Guidance, together with all other relevant circumstances, when examining the adequacy of an institution's information security program.

VI. OTS Conforming and Technical Change

OTS is making a conforming, technical change to its Security Procedures Rule at 12 CFR 568.5. That regulation currently provides that savings associations and subsidiaries that are not

---

necessary in any situation affecting the health and safety of consumers. 47 CFR 64.1200(f)(2). See also FCC Report and Order adopting rules and regulations implementing the TCPA, October 16, 1992, available at http://www.fcc.gov/cgb/donotcall/, paragraph 51 (calls from utilities to notify customers of service outages, and to warn customers of discontinuance of service are included within the exemption for emergencies). Financial institutions will give customer notice under the final Guidance for a public safety purpose, namely, to permit their customers to protect themselves where their sensitive information is likely to be misused, for example, to facilitate

functionally regulated must comply with the Security Guidelines in Appendix B to Part 570. OTS is adding a sentence to make clear that Supplement A to Appendix B is intended as interpretive guidance only.

With regard to this rule change, OTS finds that there is good cause to dispense with prior notice and comment and with the 30-day delay of effective date mandated by the Administrative Procedure Act. 5 U.S.C. 553. OTS believes that these procedures are unnecessary and contrary to the public interest because the revision merely makes conforming and technical changes to an existing provision. A conforming and technical change is necessary to make clear that Supplement A to Appendix B to Part 570 is intended as interpretive guidance only. Because the amendment in the rule is not substantive, it will not affect savings associations.

With regard to this rule change, OTS further finds that the Riegle Community Development and Regulatory Improvement Act of 1994 does not apply because the revision imposes no additional requirements and makes only a technical and conforming change to an existing regulation.

VII. Impact of Guidance

The Agencies invited comment on the potential burden associated with the customer notice provisions for financial institutions implementing the proposed Guidance. The Agencies also asked for information about the anticipated burden that may arise from the questions posed by customers who receive the notices. In addition, the proposed Guidance asked whether the Agencies should consider how the burden may vary depending upon the size and complexity of a financial institution. The Agencies also asked for information about the amount of burden, if any, the proposed Guidance would impose on service providers.

---

identity theft. Therefore, the Agencies believe that the exemption for emergency purposes likely would include customer notice that is provided by telephone using an artificial or prerecorded voice message call.

Although many commenters representing financial institutions stated that they already have a response program in place, they also noted that the Agencies had underestimated the burden that would be imposed on financial institutions and their customers by the proposed Guidance. Some commenters stated that the proposed Guidance would require greater time, expenditure, and documentation for audit and compliance purposes. Other commenters stated that the costs of providing notice and requiring a sufficient number of appropriately trained employees to be available to answer customer inquiries and provide assistance could be substantial.

Yet other commenters stated that the Agencies failed to adequately consider the burden to customers who begin to receive numerous notices of "unauthorized access" to their data. They stated that the stress to customers of having to change account numbers, change passwords, and monitor their credit reports would be enormous and could be unnecessary because the standard in the proposed Guidance would require notice when information subject to unauthorized access might be, but would not necessarily be, misused.

Some commenters maintained that the proposed Guidance would be especially burdensome for small community banks, which one commenter asserted are the lowest risk targets. These commenters stated that the most burdensome elements of the proposed Guidance would be creating a general policy, establishing procedures and training staff. They added that developing and implementing new procedures for determining when, where and how to provide notice and procedures for monitoring accounts would also be burdensome. One commenter recommended that the agencies exempt institutions with assets of under $500 million from having to comply with the Guidance.

Finally, a trade association commenter stated that the notice requirements in the proposed Guidance would impose a large burden on the nationwide consumer reporting agencies, over which they have no control and no means of recouping costs.

The Agencies have addressed the burdens identified by commenters as follows. First, the Agencies eliminated many of the more prescriptive elements of the response program described in the proposed Guidance. The final Guidance states that an institution's response program should be risk-based. It lists a number of components that the program should contain.

The final Guidance does not detail the steps that an institution should take to contain and control a security incident to prevent further unauthorized access to or use of customer information. It also does not state that an institution should secure all accounts that can be accessed using the same account number or name and password combination until such time as the institution and the customer can agree on a course of action. Instead, the final Guidance leaves such measures to the discretion of the institution and gives examples of the steps that an institution should consider, such as monitoring, freezing, or closing affected accounts. Thus, under the final Guidance a small institution may choose to close an affected account in place of monitoring the account, an element of the proposed Guidance that smaller institutions identified as potentially very costly.

Though the final Guidance still states that notification to regulators should be a part of an institution's response program, it states that notice should only be given when the institution becomes aware of an incident of unauthorized access to or use of "sensitive" customer information. This standard should result in fewer instances of notice to the regulators than under the proposed Guidance. The final Guidance also makes clear that when the security incident

involves a service provider, the institution may authorize the service provider to notify the institution's regulator.

The standard of notice to customers also has been modified to be less burdensome to institutions and their customers. The Agencies believe that under this new standard, customers will be less likely to be alarmed needlessly, and institutions will no longer be asked to prove a negative – namely, that misuse of information is unlikely to occur. In addition, the Agencies also have provided institutions with greater discretion to determine what should be contained in a notice to customers.

The Agencies do not believe that there is a basis for exempting small institutions from the Guidance. For example, many small institutions outsource functions to large service providers that have been the target of those seeking to misuse customer information. Therefore, the Agencies believe that all institutions should prepare customer response programs including customer notification procedures that can be used in the event the institution determines that misuse of its information about a customer has occurred or is reasonably possible. However, as noted above, the Agencies recognize that within the framework of the Guidance, an institution's program will vary depending on the size and complexity of the institution and the nature and scope of its activities.

Finally, to address comments relating to the potential burden on the nationwide consumer reporting agencies, as noted previously, the Guidance no longer suggests that customer notice always include advice to contact the nationwide consumer reporting agencies. The Agencies recognize that not all security breaches warrant such contacts. For example, we recognize that it may not always be in the best interest of a consumer to have a fraud alert placed in the

consumer's file because the fraud alert may have an adverse impact on the consumer's ability to obtain credit.

VIII. Regulatory Analysis

A. Paperwork Reduction Act

Certain provisions of the final Guidance contain "collection of information" requirements as defined in the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) (PRA). An agency may not conduct or sponsor, and a 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 requested comment on a proposed information collection as part of the notice requesting comment on the proposed Guidance. An analysis of the comments related to paperwork burden and commenters' recommendations is provided below. The OCC, FDIC, and OTS submitted their proposed information collections to OMB for review and approval and the collections have been approved. The Board has approved this final information collection under its delegated authority from OMB.

OCC: 1557-0227

FRB: [To be assigned]

FDIC: 3064-0145

OTS: 1550-0110

The Agencies have reconsidered the burden estimates published in the Proposed Guidance in light of the comments received asserting that the paperwork burden associated with the information collection were underestimated, and in light of measures taken by the Agencies to reduce burden in this final Guidance. The Agencies agreed to increase the estimate for the

time it will take an institution to develop notices and determine which customers should be notified. However, revisions incorporated into the final Guidance will result in the issuance of fewer notices than was originally estimated. A discussion of the comments received follows the revised estimates.

New Estimates:

OCC

Number of Respondents: 2,200

Estimated Time per Response:

Developing Notices: 24 hours x 2,200 = 52,800 hours

Notifying Customers: 29 hours x 36 = 1,044 hours

Total Estimated Annual Burden = 53,844 hours

Board

Number of Respondents: 6,692

Estimated Time per Response:

Developing Notices: 24 hours x 6,692 = 160,608 hours

Notifying Customers: 29 hours x 110 = 3,190 hours

Total Estimated Annual Burden = 163,798 hours

FDIC

Number of Respondents: 5,200

Estimated Time per Response:

Developing Notices: 24 hours x 5,200 = 124,800 hours

Notifying Customers: 29 hours x 91 = 2,639 hours

Total Estimated Annual Burden = 127,439 hours

OTS

Number of Respondents: 880

Estimated Time per Response:

Developing Notices: 24 hours x 880 = 21,120 hours

Notifying Customers: 29 hours x 15 = 435 hours

Total Estimated Annual Burden = 21,555 hours

Discussion of Comments:

The information collection in the proposed Guidance stated that financial institutions should: (1) develop notices to customers; and (2) determine which customers should receive the notices and send the notices to customers. The Agencies received various comments regarding the Agencies' burden estimates, including the estimated time per response and the number of recordkeepers involved.

Some commenters stated that the burden estimates of twenty hours to develop and produce notices and three days to determine which customers should receive notice in the proposed Guidance were too low. These commenters stated that the Guidance should include language indicating that an institution be given as much time as necessary to determine the scope of an incident and examine which customers may be affected. One of these commenters stated that ten business days, as recommended by the California Department of Consumer Affairs Office of Privacy Protection, should provide an institution with a known safe harbor to complete the steps described lest regulated entities be subject to inconsistent notification deadlines from the same incident.

These commenters misunderstood the meaning of PRA burden estimates. PRA burden estimates are judgments by Agencies regarding the length of time that it would take institutions

to comply with information collection requirements. These estimates do not impose a deadline upon institutions to complete a requirement within a specific period of time.

The final Guidance states that an institution should notify customers "as soon as possible" after an investigation leads it to conclude that misuse of customer information has occurred or is reasonably possible. It also states that notification may be delayed at the written request of law enforcement.

The cost of disclosing information is considered part of the burden of an information collection. 5 CFR 1320.3(b)(1)(ix). Many commenters stated that the Agencies had underestimated the cost associated with disclosing security incidents to customers pursuant to the proposed Guidance. However, these commenters did not distinguish between the usual and customary costs of doing business and the costs of the disclosures associated with the information collection in the proposed Guidance.

For example, one commenter stated that the Agencies' estimates did not include $0.60 per customer for a one-page letter, envelope, and first class postage; the customer service time, handling the enormous number of calls from customers who receive notice; or the costs associated with closing or reopening accounts, printing new checks or embossing new cards. This commenter stated that printing and mailing costs, alone, for one notice to its customer database, at current postal rates, would be at least $500,000.

Some of the costs mentioned in this comment are non-labor costs associated with providing disclosures. The Agencies assumed that non-labor costs associated with the disclosures would be negligible, because institutions already have in place well-developed systems for providing disclosures to their customers. This comment and any other comments

received regarding the Agencies' assumptions about non-labor costs will be taken into account in any future estimate of the burden for this collection.

Other costs mentioned in this comment, such as the cost of customer service time, printing checks, and embossing cards, are costs that the institution would incur regardless of the implementation of the final Guidance. These costs are not associated with an information collection, and, therefore, have not been factored into the Agencies' cost estimates.

In addition, the estimates in this comment are based on the assumption that notice should always be provided by mail. However, the final Guidance states that financial institutions should deliver customer notice in any manner designed to ensure that a customer can reasonably be expected to receive it, such as by telephone, mail, or electronically for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically. The Agencies assume that given this flexibility, financial institutions may not necessarily choose to mail notices in every case, but may choose less expensive methods of delivery that ensure customers will reasonably be expected to receive notice.

Another commenter concerned about the burdens imposed on consumer reporting agencies provided an example of a security breach involving a single company from which identifying information about 500,000 military families was stolen. Among other things, the company's notice to its customers advised them to contact the 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 - 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

[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."

- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Risk Assessment and Controls

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

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

---

[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.

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 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;

---

[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.

[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.

- 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 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.

---

[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 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.

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.

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.

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.

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

OCC

[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.

[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).

12 CFR part 30

Banks, banking, Consumer protection, National banks, Privacy, Reporting and recordkeeping requirements.

Board

12 CFR Part 208

Banks, banking, Consumer protection, Information, Privacy, Reporting and recordkeeping requirements.

12 CFR Part 225

Banks, banking, Holding companies, Reporting and recordkeeping requirements.

FDIC

12 CFR Part 364

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

OTS

12 CFR Part 568

Consumer protection, Privacy, Reporting and recordkeeping requirements, Savings associations, Security measures.

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.

Department of the Treasury

Office of the Comptroller of the Currency

12 CFR CHAPTER I

Authority and Issuance

For the reasons set out in the joint preamble, the OCC amends part 30 of chapter I of title 12 of the Code of Federal Regulations to read as follows:

PART 30 – SAFETY AND SOUNDNESS STANDARDS

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

Authority: 12 U.S.C. 93a, 371, 1818, 1831p, 3102(b); 15 U.S.C. 1681s, 1681w, 6801, 6805(b)(1).

2. Revise the heading of Appendix B to read "Interagency Guidelines Establishing Information Security Standards."

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

Dated: March 9, 2005

/s/

Julie L. Williams

Acting Comptroller of the Currency.