Supporting Statement for the
Recordkeeping and Disclosure Requirements Associated with the Guidance on Response Programs for Unauthorized Access to Customer Information
(FR 4100; OMB No. 7100-0309)

Summary

The Board of Governors of the Federal Reserve System, under delegated authority from the Office of Management and Budget (OMB), proposes to extend for three years, without revision, the Recordkeeping and Disclosure Requirements Associated with the Guidance on Response Programs for Unauthorized Access to Customer Information (ID-Theft Guidance; FR 4100; OMB No. 7100-0309). Recent trends in customer information theft and the accompanying misuse of that information have led to the issuance of a supplemental interpretation of existing information technology-related security guidelines applicable to financial institutions. The supplemental guidelines are designed to facilitate timely and relevant notification of affected customers and the appropriate regulatory authority (ARA) of the financial institutions. The guidelines provide specific direction regarding the nature and content of customer notice. The annual burden for the ID-Theft Guidance Requirements is estimated to be 62,135 hours.

Background and Justification

On March 29, 2005, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and National Credit Union Administration (collectively, the agencies), published the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (security guidelines) in the *Federal Register*. These security guidelines were published to fulfill a requirement in section 501(b) of the Gramm-Leach-Bliley Act (GLBA) that requires financial institutions to develop and implement information security programs designed to protect their customers' information.[1] The ID-Theft guidance, which interprets the security guidelines, describes the components of a response program and sets a standard for providing notice to customers affected by unauthorized access to or use of customer information that could result in substantial harm or inconvenience to those customers.

The ID-Theft guidance states that:

> an institution should notify affected customers when it becomes aware of unauthorized access to "sensitive customer information" unless the institution, after an appropriate investigation, reasonably concludes that misuse is unlikely to occur and takes appropriate

1 The agencies may treat an institution's failure to implement the requirements in the ID-Theft guidance as a violation of the § 501(b) guidelines or as an unsafe or unsound practice within the meaning of 12 U.S.C. 1786 or 1818.

steps to safeguard the interests of affected customers, including monitoring affected customers' accounts for unusual or suspicious activity.

For the purposes of the ID-Theft guidance, the agencies define sensitive customer information to mean a customer's social security number, personal identification number, or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access another person's account, such as user name and password.

The ID-Theft guidance provides that an expected component of a financial institution's incident response program is notifying its ARA upon becoming aware of an incident of unauthorized access to sensitive customer information. The guidance leaves the form and content of regulatory notice to the discretion of the subject financial institution. The Federal Reserve uses such notifications to monitor the institution's implementation of the guidance, and thus, enhance the supervision of individual institutions. Further, information collected from notices permit improved monitoring of security and ID-theft related trends in the industry, and thus, enhance the development of future supervisory guidance. While each agency participated in the issuance of the ID-Theft guidance, each agency independently implemented the guidance and communicated that implementation with the institutions under their respective primary jurisdiction.

Description of Information Collection

Response Program

The ID-Theft guidance describes that every financial institution develop a response program to protect against and address reasonably foreseeable risks associated with internal and external threats to the security of customer information. The ID-Theft guidance further describes the components of a response program, which includes procedures for notifying customers about incidents of unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the customer. It also provides that a financial institution is expected to expeditiously implement its response program to address incidents of unauthorized access to customer information.

A response program should contain policies and procedures that enable the financial institution to:

- Assess the situation to determine the nature and scope of the incident, and identify the information systems and types of customer information affected;
- Notify the institution's ARA and, in accordance with applicable regulations and guidance, file a Suspicious Activity Report (SAR; FR 2230; OMB No. 7100-0212) and notify appropriate law enforcement agencies;
- Take measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, including shutting down particular applications or

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

- Notify 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.

Notification Requirements

The ID-Theft guidance provides that a financial institution should notify each affected customer when it becomes aware of an incident of unauthorized access to sensitive customer information, unless the institution can reasonably conclude that the information will not be misused.

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. 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 Federal Trade Commission's (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.[2]

Time Schedule for Information Collection

2 Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are http://www.ftc.gov/bcp/edu/microsites/idtheft/ and 1-877-IDTHEFT, respectively. 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).

The ID-Theft guidance provides that a financial institution is expected to expeditiously implement its response program to address incidents of unauthorized access to customer information. The guidance provides that a financial institution should notify its designated Federal Reserve Bank upon becoming aware of an incident of unauthorized access to sensitive customer information. It also provides that a financial institution should notify each affected customer of an incident of unauthorized access to sensitive customer information when the institution determines that misuse of such information has occurred or that misuse is reasonably possible.

Sensitive Questions

This collection of information contains no questions of a sensitive nature, as defined by OMB guidelines.

Consultation Outside the Agency

Representatives from the agencies responsible for the recordkeeping and disclosure requirements associated with the guidance have reviewed their respective information collections and agreed that revisions to the collections are not necessary at this time. On March 6, 2008, the Federal Reserve published a notice in the *Federal Register* (73 FR 12176) requesting public comment for sixty days on the extension, without revision, of the ID-Theft Guidance. The comment period for this notice expired on May 5, 2008. The Federal Reserve did not receive any comments. On May 15, 2008, the Federal Reserve published a final notice in the Federal Register (73 FR 28117).

Legal Status

The Board's Legal Division has determined that the recordkeeping and disclosure requirements associated with the FR 4100 are authorized by the GLBA and are mandatory (15 U.S.C. 6801(b)). Since the Federal Reserve does not collect information associated with the FR 4100, any issue of confidentiality would not generally be an issue. However, confidentiality may arise if the Federal Reserve were to obtain a copy of a customer notice during the course of an examination or were to receive a copy of a SAR. In such cases the information would be exempt from disclosure to the public under the Freedom of Information Act (5 U.S.C 552(b)(3), (4), and (8)). Also, a federal employee is prohibited by law from disclosing a SAR or the existence of a SAR (31 U.S.C. 5318(g)).

Estimate of Respondent Burden

The ID-Theft guidance requires financial institutions to: develop notices to the customers; determine which customers should receive the notices and send the notices to the customers; and ensure that the contracts between the institutions' and service providers satisfy the ID-Theft guidance.

The total annual burden is estimated to be 62,135 hours, as shown in the following table. The estimated annual burden for this information collection is less than 1.4 percent of the total Federal Reserve System burden. The Federal Reserve estimates that it takes institutions twenty-four hours (three business days) to develop and produce the notices described in the ID-Theft guidance, eight hours to update and maintain the notice template, and twenty-nine hours per incident (three and a half business days) to determine which customers should receive the notice and notify the customers. For the purposes of this analysis, the annual burden hours associated with developing a customer notice apply only to newly created institutions. Also, it is estimated that two percent of supervised institutions will experience an incident of unauthorized access to customer information on an annual basis, resulting in customer notification.[3]

The burden estimate does not include time for financial institutions to adjust their contracts with service providers, if needed; nor for service providers to disclose information pursuant to the ID-Theft guidance.

	Number of respondents	*Estimated annual frequency*	*Estimated average hours per response*	*Estimated annual burden hours*
Develop customer notice	102	1	24	2,448
Update and maintain customer notice	6,957	1	8	55,656
Incident notification	139	1	29	4,031
Total				62,135

The total cost to the public is estimated to be $3,762,274.[4]

Estimate of Cost to the Federal Reserve System

The annual cost to the Federal Reserve System for processing this information collection is negligible.

3 This estimate is based upon the agencies' experience and data gathered by the Federal Deposit Insurance Corporation on 2,000 institutions that indicates slightly less than one percent of those institutions experienced some form of unauthorized access to customer information during any 12-month period. However, the agencies assumed that other incidents of unauthorized access to customer information may have occurred but were not reported.

4 Total cost to the public was estimated using the following formula. Percent of staff time, multiplied by annual burden hours, multiplied by hourly rate: 38% - Clerical @ $25; 39% - Managerial or Technical @ $55; 8% - Senior Management @ $100; and 15% - Legal Counsel @ $144. Hourly rate estimates for each occupational group are averages using data from the Bureau of Labor and Statistics, *Occupational Employment and Wages*, news release."