Supporting Statement for the
Reporting, 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 (Board), under delegated authority from the Office of Management and Budget (OMB), proposes to extend for three years, without revision, the Reporting, 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). The ID-Theft Guidance is an information collection associated with the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (security guidelines), which was published in the *Federal Register* in March 2005.[1] Trends in customer information theft and the accompanying misuse of that information led to the issuance of these security guidelines applicable to financial institutions. The security guidelines are designed to facilitate timely and relevant notification of an incident of unauthorized access to sensitive customer information to affected customers and the appropriate regulatory authority (ARA) of the financial institutions. The security guidelines provide specific direction regarding the development of response programs and customer notifications. The aggregate annual burden for the ID-Theft Guidance is estimated to be 14,856 hours.

Background and Justification

On March 29, 2005, the Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, the agencies), published the 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 an information security program designed to protect their customers' information.[2] The ID-Theft Guidance 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 and describes the required components of a response program for such incidents.

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

---

[1] *See* 70 FR 15736.

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

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 on to 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 ID-Theft Guidance leaves the form and content of regulatory notice to the discretion of the subject financial institution. Reserve Banks use such notifications to monitor the institution's implementation of the ID-Theft Guidance, and thus enhance the supervision of individual institutions. Further, information collected from notices permits improved monitoring of security and ID-theft related trends in the industry, and thus enhances the development of future supervisory guidance and, more generally, informs the Board's cyber security program. While each of the agencies participated in the issuance of the ID-Theft Guidance, each agency independently implemented the guidance and communicated how the guidance would be applied with the institutions under their respective primary jurisdiction.

Description of Information Collection

Response Program

The ID-Theft Guidance requires 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 include 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.

The ID-Theft Guidance 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 12 to 24 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.[3]

Time Schedule for Information Collection

[3] 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 regulated by the Board should notify its designated 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.

Legal Status

The Board's Legal Division has determined that the reporting, 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 FR 4100 provides that a financial institution regulated by the Board should notify its designated Reserve Bank upon becoming aware of an incident of unauthorized access to sensitive customer information, issues of confidentiality may arise if the Board were to obtain a copy of a customer notice during the course of an examination, a copy of a SAR, or other sensitive customer information. In such cases, the information would likely be exempt from disclosure to the public under the Freedom of Information Act (5 U.S.C § 552(b)(3), (4), (6), 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)).

Consultation Outside the Agency

Representatives from the agencies responsible for the recordkeeping and disclosure requirements associated with the ID-Theft Guidance have reviewed their respective information collections and agreed that revisions to the collections are not necessary at this time.

On September 12, 2017, the Board published a notice in the *Federal Register* (82 FR 42814) requesting public comment for 60 days on the extension, without revision, of the Reporting, Recordkeeping, and Disclosure Requirements Associated with the Guidance on Response Programs for Unauthorized Access to Customer Information. The comment period for this notice expires on November 13, 2017.

Estimate of Respondent Burden

The total annual burden for the FR 4100 is estimated to be 14,856 hours, as shown in the table below. The ID-Theft Guidance requires financial institutions to develop and maintain a response program to address unauthorized access to customer information maintained by the institution or its service providers.[4] Based on 2016 data, staff estimates that 1 new institution per

[4] GLBA defines Board-regulated institutions as: State member banks (SMBs), bank holding companies (BHCs), affiliates and certain non-bank subsidiaries of bank holding companies, uninsured state agencies and branches of foreign banks, commercial lending companies owned or controlled by foreign banks, and Edge and agreement corporations. Based on the Board of Governors of the Federal Reserve System 103rd Annual Report 2016 there are: 5,052 U.S. BHCs, 829 state member banks, 219 branches & agencies of foreign banks, 1 commercial lending

year would take, on average, 24 hours to develop its response program. On a continuing basis, burden associated with maintenance of the response program is considered negligible. For each qualifying incident the ID-Theft Guidance requires financial institutions to prepare and send notices to its federal regulator, affected customers, and service providers. The Board estimates that 412 financial institutions[5] would take on average 36 hours per incident to prepare and send notifications.[6] The recordkeeping and disclosure requirements represent less than 1 percent of total Federal Reserve System paperwork burden.

	Number of respondents[7]	*Annual frequency*	*Estimated average hours per response*	*Estimated annual burden hours*
Recordkeeping:				
Develop response program	1	1	24	24
Reporting and Disclosure:				
Incident notification	412	1	36	14,832
Total				14,856

The total cost to the public is estimated to be $815,594.[8]

Sensitive Questions

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

company, and 42 edge and agreement corporations. For purposes of the ID-Theft Guidance, the Board is the ARA for these entities.

[5] Based on data from the Federal Reserve System Security Incident Notification System (SINS) database, Supervision & Regulation staff determined that during 2016, 152 SMBs and 260 BHCs filed incident notifications with the Federal Reserve System, affected customers, and service providers.

[6] Per the March 29, 2005, Federal Register notice, the Board considers incident notification to be the responsibility of the financial institution. If the financial institution chooses to have a service provider disclose information on their behalf that burden is considered part of Incident Notification as shown in the burden table.

[7] Of these respondents, 22 are considered small entities as defined by the Small Business Administration (i.e., entities with less than $550 million in total assets) https://www.sba.gov/contracting/getting-started-contractor/make-sure-you-meet-sba-size-standards/table-small-business-size-standards.

[8] Total cost to the public was estimated using the following formula: percent of staff time, multiplied by annual burden hours, multiplied by hourly rates (30% Office & Administrative Support at $18, 45% Financial Managers at $67, 15% Lawyers at $67, and 10% Chief Executives at $93). Hourly rates for each occupational group are the (rounded) mean hourly wages from the Bureau of Labor and Statistics (BLS), Occupational Employment and Wages May 2016, published March 31, 2017 http://www.bls.gov/news.release/ocwage.t01.htm. Occupations are defined using the BLS Occupational Classification System, www.bls.gov/soc/.

Estimate of Cost to the Federal Reserve System

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