

**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. to be obtained)**

**Summary**

The Board of Governors of the Federal Reserve System, under delegated authority from the Office of Management and Budget (OMB), proposes to implement 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. to be obtained). The Paperwork Reduction Act (PRA) classifies reporting, recordkeeping, or disclosure requirements as an “information collection.”<sup>1</sup> The PRA requires the Federal Reserve to renew authority for information collections every three years.

On August 12, 2003, the federal financial banking agencies (the Agencies)<sup>2</sup> published a notice in the *Federal Register* seeking comment on the proposed guidance. In addition, as part of the Agencies’ continuing efforts to reduce paperwork burden, the Agencies invited comments on the burden associated with the proposed information collection.

**Background and Justification**

In February 2001, the agencies published the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (security guidelines). These security guidelines were published to fulfill a requirement in section 501(b) of the Gramm-Leach-Bliley Act (GLBA), that require financial institutions to implement information security programs designed to protect their customers’ information.<sup>3</sup> The proposed 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 proposed ID-Theft guidance states that “an institution should notify affected customers when it becomes aware of unauthorized access to *sensitive customer*

---

<sup>1</sup> 44 U.S.C. § 3501 *et seq.*

<sup>2</sup> For the purposes of this document the agencies include: the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA).

<sup>3</sup> The Agencies may treat an institution’s failure to implement the requirements in the final 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.

*information*<sup>4</sup> 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.”

## **Description of Information Collection**

The proposed ID-Theft guidance sets forth the Agencies' expectations for the creation of response programs and customer notifications.

**Response Program.** The proposed ID-Theft guidance describes the Agencies' expectations 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 proposed 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 primary Federal regulator 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
- Address and mitigate harm to individual customers.

**Notification Requirements.** The proposed 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.

---

<sup>4</sup> For the purposes of the proposed ID-Theft guidance, the Agencies define *sensitive customer information* to mean a customer's social security number, personal identification number (PIN), or account number, in conjunction with a personal identifier, such as the individual's name, address, or telephone number. *Sensitive customer information* would also include 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 customer notices should include a general description of the incident and provide information to assist customers in mitigating potential harm. This information should including a customer service number, steps customers can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

In addition, institutions are expected to inform each customer about the availability of the Federal Trade Commission's (FTCs) online guidance regarding measures to protect against identity theft and to encourage the customer to report any suspected incidents of identity theft to the FTC. Institutions should also provide customers with the FTCs website ([www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)) and the identity theft toll free number (877-IDTHEFT).

### **Time Schedule for Information Collection**

The proposed 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. It also provides that a financial institution should notify each affected customer when it becomes aware of an incident of unauthorized access to *sensitive customer information*.

### **Legal Status**

The Board's Legal Division has determined that the recordkeeping and disclosure requirements associated with the new FR 4100 are authorized by the GLBA and are mandatory (15 U.S.C. 6801 and 6805). Since the Board 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 Board 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)(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)).

### **Consultation Outside the Agency**

In implementing the ID-Theft guidance to interpret the security guidelines, the Agencies' have jointly published the proposal for comment in the *Federal Register*. Public comments are requested by October 14, 2003.

### **Estimate of Respondent Burden**

The information collections in the proposed ID-Theft guidance would require 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 proposed ID-Theft guidance.

The Agencies' jointly estimated that it will initially take institutions 20 hours (2.5 business days) to develop and produce the notices described in the proposed ID-Theft guidance and 24 hours per incident (three business days) to determine which customers should receive the notice and notify the customers. For the purposes of this analysis, 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.<sup>5</sup>

Thus, the burden associated with this collection of information may be summarized in the table below. However, 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 proposed ID-Theft guidance.

	<i>Number of respondents</i>	<i>Estimated annual frequency</i>	<i>Estimated response time</i>	<i>Estimated annual burden hours</i>
Develop notice	6,692	1	20 hours	133,840
Customer notification	134	1	24 hours	3,216
<i>Total</i>				137,056

Based on a rate of \$20 per hour, the estimated cost to the public for this information collection is \$2,741,120.

### **Sensitive Questions**

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

### **Estimate of Cost to the Federal Reserve System**

Since the Federal Reserve does not collect any information, the cost to the Federal Reserve System is negligible.

<sup>5</sup> This estimate is based upon the Agencies' experience and data gathered by the FDIC 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 are assuming that other incidents of unauthorized access to customer information may have occurred but were not reported.