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

Summary

The Board of Governors of the Federal Reserve System (Board), under authority delegated by the Office of Management and Budget (OMB), has extended for three years, without revision, the Reporting, Recordkeeping, and Disclosure Provisions Associated with the Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (FR 4100; OMB No. 7100-0309). The FR 4100 is the Board's information collection associated with the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (ID-Theft Guidance). The ID-Theft Guidance was published in the *Federal Register* in March 2005.[1] The ID-Theft Guidance, which applies to financial institutions, was issued in response to developing trends in the theft and accompanying misuse of customer information. The Guidance includes certain voluntary reporting, recordkeeping, and disclosure provisions.

The estimated total annual burden for the FR 4100 is 12,120 hours. There is no formal reporting form for this information collection.

Background and Justification

On February 1, 2001, the Board, Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS)[2] (collectively, the agencies) published the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Security Guidelines),[3] which were published to fulfill a requirement in section 501(b) of the Gramm-Leach-Bliley Act (GLBA) that requires the agencies to establish appropriate standards for financial institutions to develop and implement an information security program designed to protect their customers' information. The Security Guidelines state that an institution should consider implementing a response program that specifies actions to be taken when an institution suspects or detects that unauthorized individuals have gained access to customer information systems. To address the need for additional interpretive guidance regarding section 501(b) of GLBA and the Security Guidelines, on March 29, 2005, the agencies adopted the ID-Theft Guidance. The ID-Theft Guidance sets forth guidelines for how financial institutions should provide notice to customers affected by unauthorized access to or use of customer information that could result in substantial harm or

---

[1] See 70 FR 15736 (March 29, 2005), available at https://www.federalregister.gov/documents/2005/03/29/05-5980/interagency-guidance-on-response-programs-for-unauthorized-access-to-customer-information-and.

[2] The Dodd-Frank Wall Street Reform and Consumer Protection Act transferred the powers and duties of the OTS to the Board, FDIC, Consumer Financial Protection Bureau, and OCC, and the OTS was abolished.

[3] See 66 FR 8615 (February 1, 2001). The agencies subsequently renamed the Interagency Guidelines Establishing Standards for Safeguarding Customer Information as the Interagency Guidelines Establishing Information Security Standards.

inconvenience to those customers and describes the suggested components of a response program for such incidents.

The ID-Theft Guidance states that an institution should notify affected customers as soon as possible when it becomes aware of unauthorized access to "sensitive customer information" if the institution determines that misuse of its information about a customer has occurred or is reasonably possible and should take appropriate 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, driver's license number, account number, credit or debit card number, or a personal identification number or password, 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 the customer's account, such as username and password.

The ID-Theft Guidance provides that a suggested component of a financial institution's incident response program is notifying its appropriate regulatory authority (ARA) upon becoming aware of an incident of unauthorized access to or use of 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 financial institutions, 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. This information is not available from other sources.

Description of Information Collection

Reporting - Incident Notification

The ID-Theft Guidance provides that a financial institution regulated by the Board should notify the Federal Reserve upon becoming aware of an incident of unauthorized access to sensitive customer information. This notice may be submitted to the appropriate Reserve Bank.

Disclosure - Incident Notification

The ID-Theft Guidance provides that a financial institution should notify each affected customer as soon as possible when it becomes aware of an incident of unauthorized access to sensitive customer information if the institution determines that misuse of its information about a customer has occurred or is reasonably possible.

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 website address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.[4]

The ID-Theft Guidance also encourages 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.[5]

Recordkeeping - Develop Response Program

The Security Guidelines require that every financial institution consider developing a written 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 suggested 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,

[4] Currently, the FTC website for ID Theft information is https://consumer.ftc.gov/features/identity-theft. The institution may also refer customers to any materials developed pursuant to section 151(b) of the Fair and Accurate Credit Transactions Act (FACT Act), which are educational materials developed by the FTC to teach the public how to prevent identity theft.

[5] Nationwide reporting agencies include companies like Experian, Equifax, and TransUnion.

- Notify the institution's ARA and, in accordance with applicable regulations and guidance, file a Suspicious Activity Report (SAR; OMB No. 1506-0065) and notify appropriate law enforcement agencies,
- Take 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, and
- Notify customers when warranted.

Under the ID-Theft Guidance, where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is suggested that the financial institution notify the institution's customers and ARA. However, an institution may authorize or contract with its service provider to notify the institution's customers or ARA on its behalf.

Respondent Panel

The FR 4100 panel comprises the following Board-regulated financial institutions: state member banks, bank holding companies (BHCs), affiliates and certain non-banking subsidiaries of BHCs, uninsured state agencies and branches of foreign banks, commercial lending companies owned or controlled by foreign banks, savings and loan holding companies, and Edge and agreement corporations.

Frequency and Time Schedule

The FR 4100 is event generated, conducted as incidents occur. 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 the Federal Reserve 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.

Public Availability of Data

There are no data related to this information collection available to the public.

Legal Status

FR 4100 is authorized by section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801(b)), which requires the Board, FDIC, and OCC to establish appropriate standards for financial institutions to develop and implement an information security program designed to protect their customers' information and a response program that specifies actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to

customer information systems. Because the provisions under FR 4100 are contained in guidance, which is nonbinding,[6] the provisions are voluntary.

The disclosure provisions of FR 4100 are not confidential; those provisions advise banking organizations to disclose certain information regarding data security breaches to certain parties, including their primary federal regulator (or concern disclosures by third-party service providers to banking organizations), without specifying the confidential treatment of this information. To the extent the Board receives disclosure notices from banking organizations according to the recommendations set out in FR 4100, records relating to these notices would be records subject to the Freedom of Information Act (FOIA). However, these records would be considered confidential pursuant to exemption 8 of the FOIA, which protects information contained in "examination, operating, or condition reports" obtained in the bank supervisory process (5 U.S.C. § 552(b)(8)). In addition, the information obtained by the Board under FR 4100 may, depending on the banking organization's treatment of the submitted information, also be kept confidential under exemption 4 of the FOIA, which protects commercial or financial information that is obtained from a person and is privileged or confidential (5 U.S.C. § 552(b)(4)).

FR 4100 also contains certain recordkeeping provisions that require banking organizations to maintain certain records. These records would only be subject to the FOIA to the extent that the Board obtained such records as part of the examination or supervision of a banking organization. If obtained by the Board, this information would fall under the same exemptions as the Board's records regarding banking organizations' disclosure notifications. Exemption 8, which protects information contained in "examination, operating, or condition reports" obtained in the bank supervisory process, would apply (5 U.S.C. § 552(b)(8)), as would exemption 4, which protects commercial or financial information that is obtained from a person and is privileged or confidential (5 U.S.C. § 552(b)(4)).

Consultation Outside the Agency

There has been no consultation outside the Federal Reserve System with respect to the extension, without revision, of the FR 4100.

Public Comments

On September 28, 2023, the Board published an initial notice in the *Federal Register* (88 FR 66845) requesting public comment for 60 days on the extension, without revision, of the FR 4100. The comment period for this notice expired on November 27, 2023. The Board did not receive any comments. The Board adopted the extension, without revision, of the FR 4100 as originally proposed. On February 16, 2024, the Board published a final notice in the *Federal Register* (89 FR 12343).

[6] See 12 CFR 262.7; 12 CFR 262 Appendix A, Statement Clarifying the Role of Supervisory Guidance (April 8, 2021).

Estimate of Respondent Burden

As shown in the table below, the estimated total annual burden for the FR 4100 is 12,120 hours. The Security Guidelines require financial institutions to develop and maintain a response program to address unauthorized access to customer information maintained by the institution or its service providers, and the ID-Theft Guidance sets forth the suggested components of such a program. The Board estimates that 1 new institution per year would take 30 hours on average to develop its response program. On a continuing basis, burden associated with maintenance of the response program is considered negligible. For each incident of unauthorized access to or use of customer information, the ID-Theft Guidance suggests that a financial institution prepare and send a notice to its federal regulator, affected customers, and service providers. The Board estimates that financial institutions[7] will prepare and send 390 notifications per year, with an estimated 31 hours per incident.[8] The burden estimate was produced using the standard Board burden calculation methodology. These reporting, recordkeeping, and disclosure provisions represent less than 1 percent of the Board's total paperwork burden.

FR 4100	*Estimated number of respondents*[9]	*Estimated annual frequency*	*Estimated average hours per response*	*Estimated annual burden hours*
Reporting				
Incident notification to the Board	390	1	1	390
Recordkeeping				
Develop response program	1	1	30	30
Disclosure				
Incident notification to customers and service providers	390	1	30	11,700
Total				12,120

[7] Based on data from the Federal Reserve System Cyber Event Repository (CER) database, Supervision and Regulation staff determined that from 2020-2022, an average of 390 applicable incident notifications were filed each year with the Federal Reserve System, affected customers, and service providers.

[8] 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.

[9] Of these respondents, 36 are considered small entities as defined by the Small Business Administration (i.e., entities with less than $850 million in total assets). Size standards effective March 17, 2023. See https://www.sba.gov/document/support-table-size-standards. There are no special accommodations given to mitigate the burden on small institutions. When promulgating the Guidance, the agencies determined not to exempt small institutions from the Guidance. However, the agencies noted that an institution's program will vary depending on the size and complexity of the institution and the nature and scope of its activities.

The estimated total annual cost to the public for the FR 4100 is $802,950.[10]

Sensitive Questions

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

Estimate of Cost to the Federal Reserve System

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

[10] Total cost to the responding public is estimated using the following formula: total burden hours, multiplied by the cost of staffing, where the cost of staffing is calculated as a percent of time for each occupational group multiplied by the group's hourly rate and then summed (30% Office & Administrative Support at $22, 45% Financial Managers at $80, 15% Lawyers at $79, and 10% Chief Executives at $118). Hourly rates for each occupational group are the (rounded) mean hourly wages from the Bureau of Labor Statistics (BLS), *Occupational Employment and Wages, May 2022*, published April 25, 2023, https://www.bls.gov/news.release/ocwage.t01.htm. Occupations are defined using the BLS Standard Occupational Classification System, https://www.bls.gov/soc/.