Supporting Statement for the
Computer-Security Incident Notification
(FR 2231; OMB No. 7100-0384)

Summary

The Board of Governors of the Federal Reserve System (Board), under authority delegated by the Office of Management and Budget (OMB), proposes to extend for three years, without revision, the Computer-Security Incident Notification (FR 2231; OMB No. 7100-0384). A banking organization is required to notify its primary Federal banking regulator of any "computer-security incident" that rises to the level of a "notification incident," as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. A bank service provider is required to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident, that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

The estimated total annual burden for the FR 2231 is 285 hours. There is no formal reporting form for this information collection.

Background and Justification

Computer-security incidents can result from destructive malware or malicious software (cyberattacks), as well as non-malicious failure of hardware and software, personnel errors, and other causes. Cyberattacks targeting the financial services industry have increased in frequency and severity in recent years.[1] These cyberattacks can adversely affect banking organizations' networks, data, and systems, and ultimately their ability to resume normal operations.

Given the frequency and severity of cyberattacks on the financial services industry, the Board, Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) (collectively, the agencies) published a final rule on November 23, 2021, in which the agencies set out requirements that a banking organization's primary Federal regulator be notified as soon as possible of a computer-security incident[2] that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, the viability of the banking organization's operations, result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector.[3] Timely notification is important as it allows the agencies to (1) have early awareness of emerging threats to banking organizations and the broader financial system, (2) better assess the threat a notification incident poses to a banking organization and take appropriate actions to address the threat, (3) facilitate and approve requests

---

[1] See, e.g., Financial Crimes Enforcement Network, *SAR Filings by Industry* (January 1, 2014 - December 31, 2022) (last accessed March 4, 2024), https://www.fincen.gov/reports/sar-stats/sar-filings-industry. (Trend data may be found by viewing the Excel file "Depository Institution" and selecting the tab marked "Exhibit 5.").

[2] A computer-security incident is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. See 12 CFR 225.301(b)(4).

[3] These computer-security incidents may include major computer-system failures; cyber-related interruptions, such as distributed denial of service and ransomware attacks; or other types of significant operational interruptions.

from banking organizations for assistance through U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP),[4] (4) provide information and guidance to banking organizations, and (5) conduct horizontal analyses to provide targeted guidance and adjust supervisory programs.

Other related reporting requirements do not sufficiently account for the risks posed by all computer-security incidents. Notification under the Bank Secrecy Act[5] and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[6] provide the agencies with awareness of certain computer-security incidents. Nonetheless, these notification standards do not cover all computer-security incidents of which the agencies, as supervisors, need to be alerted and would not always result in timely notification to the agencies.

Description of Information Collection

The FR 2231 is comprised of a reporting requirement in section 225.302 and a disclosure requirement in section 225.303 of the Board's Regulation Y - Bank Holding Companies and Change in Bank Control (12 CFR Part 225).

Reporting Requirement

Section 225.302 requires a banking organization to notify the appropriate Board-designated point of contact about a notification incident through email, telephone, or other similar methods that the Board may prescribe. The Board has designated the email incident@frb.gov and the telephone number (866) 364-0096 as the two options for submitting a notification incident. The Board must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred.[7]

Disclosure Requirement

---

[4] OCCIP coordinates with U.S. Government agencies to provide agreed-upon assistance to banking and other financial services sector organizations on computer-incident response and recovery efforts. These activities may include providing remote or in-person technical support to an organization experiencing a significant cyber event to protect assets, mitigate vulnerabilities, recover and restore services, identify other entities at risk, and assess potential risk to the broader community. The Federal Financial Institutions Examination Council's Cybersecurity Resource Guide for Financial Institutions (September 2022) identifies additional information available to banking organizations. Available at: https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf.

[5] See 31 U.S.C. § 5311 et seq.; 31 CFR Subtitle B, Chapter X.

[6] See 15 U.S.C. § 6801; 12 CFR Part 30, Appendix B, Supplement A (OCC); 12 CFR Part 208, Appendix D-2, Supplement A, 12 CFR 211.5(l), 12 CFR Part 225, Appendix F, Supplement A (Board); 12 CFR Part 364, Appendix B, Supplement A (FDIC).

[7] 5 CFR 1320.(d)(2) states that agencies must demonstrate a substantial need for a collection that requires responses more often than quarterly and/or requiring a response in fewer than 30 days from receipt of a request. The Board notes that due to this collection being in response to incidents, which are unpredictable, respondents may have to submit information more often than quarterly. Further, to ensure timely transfer of information, respondents are required to notify the Board-designated contact in fewer than 30 days from the time of the incident.

Section 225.303 requires a bank service provider to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. A bank-designated point of contact is an email address, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer. If the banking organization customer has not previously provided a bank-designated point of contact, such notification shall be made to the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means. The notification requirement does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer.[8]

For both requirements, the Board understands that respondents may use information technology (email) to comply.

Respondent Panel

The FR 2231 panel comprises banking organizations for which the Board serves as primary regulator, which are U.S. bank holding companies, U.S. savings and loan holding companies, state member banks, U.S. operations of foreign banking organizations, Edge or agreement corporations, and bank service providers, which are defined as bank service companies or other persons that perform services subject to the Bank Service Company Act. No designated financial market utility is considered a banking organization for the purposes of this collection.

Frequency and Time Schedule

Banking organizations must notify the appropriate Board-designated point of contact about a notification incident as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. A bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

Public Availability of Data

No data collected by this information collection are published.

[8] 5 CFR 1320.(d)(2) states that agencies must demonstrate a substantial need for a collection which requires responses more often than quarterly and/or requiring a response in fewer than 30 days from receipt of a request. The Board notes that due to this collection being in response to incidents, which are unpredictable, respondents may have to submit information more often than quarterly. Further, to ensure timely transfer of information, respondents are required to notify the Bank-designated points of contact in fewer than 30 days from the time of the incident.

Legal Status

The FR 2231 is authorized by different statutory provisions for different covered banking organizations and bank service providers. Sections 9(6) and 11(a), 25, and 25A of the Federal Reserve Act authorize the FR 2231 with respect to state member banks, agreement corporations, and Edge corporations, respectively.[9] The FR 2231 is authorized by section 5(c) of the Bank Holding Company Act for bank holding companies and by section 10(b)(2) of the Home Owners' Loan Act for savings and loan holding companies.[10] Sections 7(c), 8(a), and 13(a) of the International Banking Act provides authority with respect to the U.S. operations of foreign banking organizations.[11] Finally, section 7(c) and (d) of the Bank Service Company Act authorizes the FR 2231 with respect to bank service providers.[12]

Information submitted to the Board pursuant to the FR 2231's reporting requirement is generally nonpublic commercial or financial information, which is both customarily and actually treated as private by the respondent. The Board therefore generally keeps such information confidential pursuant to exemption 4 of the Freedom of Information Act ("FOIA").[13] Notifications to the Board pursuant to the FR 2231's reporting requirement may also contain information contained in or related to an examination of a financial institution. Such information would be kept confidential under exemption 8 of FOIA, which protects information contained in "examination, operating, or condition reports" obtained in the bank supervisory process.[14]

Notifications required of bank service providers to their banking organization customers under the FR 2231's disclosure requirements are generally not provided to the Board, and the FOIA would only be implicated if the Board obtained such records as part of the examination or supervision of a banking organization. In the event the records are obtained by the Board as part of an examination or supervision of a financial institution, this information is considered confidential pursuant to exemption 8 of FOIA.[15] In addition, to the extent such information constitutes commercial or financial information that is both customarily and actually treated as private by the respondent, such information may also be kept confidential under exemption 4 for the FOIA.[16]

Consultation Outside the Agency

The OCC and FDIC were consulted as part of the clearance process for this information collection.

Public Comments

[9] 12 U.S.C. §§ 324 & 248(a) (state member banks), 602 (agreement corporations), and 625 (Edge corporations).
[10] 12 U.S.C. §§ 1844(c) (bank holding companies), 1467a(b)(2) (savings and loan holding companies).
[11] 12 U.S.C. §§ 3105(c)(2), 3106(a), and 3108(a).
[12] 12 U.S.C. § 1867(c)–(d).
[13] 5 U.S.C. § 552(b)(4).
[14] 5 U.S.C. § 552(b)(8).
[15] *Id.*
[16] 5 U.S.C. § 552(b)(4).

On December 6, 2024, the Board published an initial notice in the *Federal Register* (89 FR 96979) requesting public comment for 60 days on the extension, without revision, of the FR 2231. The comment period for this notice expires on February 4, 2025.

Estimate of Respondent Burden

As shown in the table below, the estimated total annual burden for the FR 2231 is 285 hours. The Board reviewed information submitted by banking organizations from May 2022 through April 2024 to estimate the number of respondents. The Board estimates that it will take up to 3 hours each to comply with the reporting and disclosure requirements. These reporting and disclosure requirements represent less than 1 percent of the Board's total paperwork burden.

FR 2231	*Estimated number of respondents* [17]	*Estimated annual frequency*	*Estimated average hours per response*	*Estimated annual burden hours*
Reporting Section 225.302	21	1	3	63
Disclosure Section 225.303	74	1	3	222
Total				285

The estimated total annual cost to the public for the FR 2231 is $19,907.[18]

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

[17] Of the reporting section respondents, 5 respondents 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. The Board is currently unable to estimate the number of bank service providers disclosure section that are small due to the varying types of banking organizations that may enter into outsourcing arrangements with bank service providers. There are no special accommodations given to mitigate the burden on small institutions.

[18] 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 $23, 45% Financial Managers at $84, 15% Lawyers at $85, and 10% Chief Executives at $124). Hourly rates for each occupational group are the (rounded) mean hourly wages from the Bureau of Labor Statistics (BLS), *Occupational Employment and Wages, May 2023*, published April 3, 2024, https://www.bls.gov/news.release/ocwage.t01.htm. Occupations are defined using the BLS Standard Occupational Classification System, https://www.bls.gov/soc/.