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

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Docket No. R-1736) (RIN 7100-AG06)

Summary

The Board of Governors of the Federal Reserve System (Board), under authority delegated by the Office of Management and Budget (OMB), has implemented the Computer-Security Incident Notification (FR 2231; OMB No. 7100-NEW). The FR 2231 covers the information collections included in a final rule (Final Rule) promulgated by the Board, Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC) (collectively, the agencies) on November 23, 2021. The Final Rule requires a banking organization 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. The banking organizations for which the Board serves as primary Federal banking regulator for the purposes of the Final Rule are U.S. bank holding companies, U.S. savings and loan holding companies, state member banks, U.S. operations of foreign banking organizations, and Edge or agreement corporations. The Final Rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced an unplanned computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours. The FR 2231 compliance date is May 1, 2022.

The estimated total annual burden for the FR 2231 is 2,502 hours. There is no formal reporting form for this information collection (the FR 2231 designation is for internal purposes only).

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 agencies believe that it is important that a banking organization's primary Federal regulator be

[1] See, e.g., Financial Crimes Enforcement Network, *SAR Filings by Industry* (January 1, 2014 - December 31, 2020) (last accessed October 11, 2021), https://www.fincen.gov/reports/sar-stats/sar-filings-industry. (Trend data may be found by downloading the Excel file "Depository Institution" and selecting the tab marked "Exhibit 5.").

notified as soon as possible of a significant computer-security incident[2] that disrupts or degrades, or is reasonably likely to 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] The Final Rule refers to these significant computer-security incidents as "notification incidents."[4] Timely notification is important as it would allow 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 from banking organizations for assistance through U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP),[5] (4) provide information and guidance to banking organizations, and (5) conduct horizontal analyses to provide targeted guidance and adjust supervisory programs.

Current reporting requirements do not sufficiently account for the risks posed by notification incidents. Notification under the Bank Secrecy Act[6] and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[7] 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.

---

[2] As defined by the Final Rule, 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. To promote uniformity of terms, the agencies have sought to align this term generally with an existing definition from the National Institute of Standards and Technology (NIST). See NIST, Computer Security Resource Center, Glossary (last accessed September 20, 2021), available at https://csrc.nist.gov/glossary/term/Dictionary.

[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.

[4] As defined in the Final Rule, a notification incident is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's (1) ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business, (2) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value, or (3) operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

[5] 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 (October 2018) identifies additional information available to banking organizations. Available at: https://www.ffiec.gov/press/pdf/FFIEC Cybersecurity Resource Guide for Financial Institutions.pdf (last accessed October 15, 2021).

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

[7] 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).

Description of Information Collection

The Final Rule, which amended the Board's Regulation Y - Bank Holding Companies and Change in Bank Control (12 CFR Part 225), contains a reporting requirement found in section 225.302 and a disclosure requirement found in section 225.303.

Reporting Requirements

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 designates the email and telephone number to be contacted in an SR letter but has not prescribed any other notification methods to this point. 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.

Disclosure Requirements

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.

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, and Edge or agreement corporations; and bank service providers, which are defined as bank service companies or other persons that performs services subject to the Bank Service Company Act. No designated financial market utility is considered a banking organization for the purposes of this collection.

Time Schedule for Information Collection

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 is published.

Legal Status

The FR 2231 is authorized pursuant to the Federal Reserve Act for state member banks, Edge corporations, and agreement corporations (12 U.S.C. §§ 321-338a), the Bank Holding Company Act of 1956 for bank holding companies (12 U.S.C. § 1844(b)), the Home Owners' Loan Act for savings and loan holding companies (12 U.S.C. § 1467a(g)), the Bank Service Company Act for bank service providers (12 U.S.C. §§ 1861-1867), and the International Banking Act of 1978 for U.S. operations of foreign banking organizations (12 U.S.C. § 3101 et seq.). The obligation to respond to the FR 2231 is mandatory.

Information disclosed to the Board pursuant to the FR 2231 reporting requirement is nonpublic commercial or financial information, which is both customarily and actually treated as private by the respondent. The Board therefore keeps such information confidential pursuant to exemption 4 of the Freedom of Information Act (FOIA) (5 U.S.C. § 552(b)(4)). Notifications to the Board pursuant to the FR 2231 reporting requirement may also contain information contained in or related to an examination of a financial institution, which would be kept confidential under exemption 8 of the FOIA (5 U.S.C. § 552(b)(8)).

Notifications to banking organization customers required under the FR 2231 disclosure requirements would generally not be 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 the FOIA, which protects information contained in "examination, operating, or condition reports" obtained in the bank supervisory process. In addition, the information may also be kept confidential under exemption 4 for the FOIA, which protects public commercial or financial information that is both customarily and actually treated as private by the respondent, or exemption 6 of the FOIA, which protects personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy (5 U.S.C. § 552(b)(6)).

Consultation Outside the Agency

This information collection was developed in conjunction with the OCC and FDIC.

Public Comments

On January 12, 2021, the agencies published a notice of proposed rulemaking in the *Federal Register* (86 FR 2299) requesting public comment on the implementation of the FR 2231. The comment period for this notice expired on April 12, 2021. The agencies received one Paperwork Reduction Act related comment which agreed that the proposed information collection has practical utility. On November 23, 2021, the agencies published a final rule in the *Federal Register* (86 FR 66424). The final rule is effective April 1, 2022, and has a compliance date of May 1, 2022.

Estimate of Respondent Burden

As shown in the table below, the estimated total annual burden for the FR 2231 is 2,502 hours. The agencies reviewed available supervisory data and Suspicious Activity Reports (SARs) involving cyber incidents against banking organizations in 2019 and 2020 to estimate the number of notification incidents expected to be reported annually. This calculation relied on descriptive criteria (e.g., ransomware, trojan, zero day, etc.) that may be indicative of the type of material computer-security incident that would meet the notification incident reporting criteria. Based on this review, the agencies estimate that approximately 150 notification incidents occurred annually, but acknowledge that the number of such incidents could increase in the future. Of these 150 incidents, the 32 are estimated to be from Board-regulated banking organizations.[8] The agencies do not have data on the exact number of affected bank service providers nor the frequency of incidents that would require bank service providers to notify their banking organization customers.[9] For both the reporting and the disclosure requirement, the agencies estimate it will take up to 3 hours 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.

[8] The number of respondents for the reporting requirement is based on allocating the estimated 150 notification incidents among the agencies based on the percentage of entities supervised by each agency. The FDIC represents the majority of the banking organizations (64 percent), while the Board supervises approximately 21 percent of the banking organizations, with the OCC supervising the remaining 15 percent of banking organizations.

[9] The number of respondents for the disclosure requirement is based on an assumption of an approximately 2 percent per year frequency of incidents from 120,392 firms, which is divided equally among the Board, OCC, and FDIC. The number of 120,392 firms is the number of firms in the United States under NAICS code 5415 in 2018, the latest year for which such data is available. See U.S. Census Bureau, *2018 SUSB Annual Data Tables by Establishment Industry*, https://www.census.gov/data/tables/2018/econ/susb/2018-susb-annual.html (last revised August 27, 2021).

FR 2231	*Estimated number of respondents*[10]	*Annual frequency*	*Estimated average hours per response*	*Estimated annual burden hours*
Reporting Section 225.302	32	1	3	96
Disclosure Section 225.303	802	1	3	2,406
Total				2,502

The estimated total annual cost to the public for the FR 2231 is $151,246.[11]

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

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

[10] Of these respondents, 22 are considered small entities as defined by the Small Business Administration (i.e., entities with less than $600 million in total assets), https://www.sba.gov/document/support--table-size-standards. The Board is currently unable to estimate the number of bank service providers 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.

[11] 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 $21, 45% Financial Managers at $74, 15% Lawyers at $71, and 10% Chief Executives at $102). 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 2021*, published March 31, 2022, https://www.bls.gov/news.release/ocwage.t01.htm. Occupations are defined using the BLS Standard Occupational Classification System, https://www.bls.gov/soc/.