SUPPORTING STATEMENT
Computer Security Incident Notification
(OMB Control No. 3064-NEW)

INTRODUCTION

The Federal Deposit Insurance Corporation (FDIC) is requesting OMB approval of a new information collection related to a final rule (rule) that requires a banking organization to provide its primary federal regulator with prompt notification of any "computer-security incident" that rises to the level of a "notification incident" as defined in the rule. The rule requires such notification upon the occurrence of a notification incident as soon as possible and no later than 36 hours after the banking organization has determined that the incident occurred. This notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator and is not intended to provide an assessment of the incident. The rule allows a banking organization to authorize or contract with a bank service provider to allow the bank service provider to make the relevant notifications to the banking organization's primary federal regulator on the banking organization's behalf.

A. JUSTIFICATION

1. Circumstances that make the collection necessary:

Internet crime and cyberattacks reported to federal law enforcement have increased in frequency and severity in recent years.[1] These types of attacks may use destructive malware or other cybersecurity exploits to target weaknesses in the computers or networks of banking organizations supervised by the agencies.[2] Some exploits have the potential to alter, delete, or otherwise render a banking organization's data and systems unusable. Depending on the scope of an incident, a banking organization's data and system backups may also be affected, which can severely affect its ability to recover operations. In addition, banking organizations have become increasingly reliant on bank service providers to provide essential technology-related products and services. These bank service providers are also vulnerable to cyber threats.

The agencies believe that it is critically important that the primary federal regulator of a banking organization be notified as soon as possible of a significant "computer-security incident"[3] that could prevent the banking organization from carrying out banking

1 *See* Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* at 5 (last accessed Sept. 4, 2020), *available at https://pdf.ic3.gov/2019_IC3Report.pdf.*
2 *See Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic: Virtual Hearing Before the Subcommittee on National Security, International Development and Monetary Policy of the U.S. House Committee on Financial Services 116th Congress* (2020) *(*written statement of Tom Kellerman, Head of Cybersecurity Strategy, VMware, Inc.), *available at https://financialservices.house.gov/uploadedfiles/hhrg-116-ba10-wstate-kellermannt-20200616.pdf*.
3 As defined by the rule, a *computer-security incident* is an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. To promote uniformity of terms, the agencies have sought to align this term to the fullest extent possible with an existing definition from the National Institute of Standards and Technology (NIST). *See*

operations, result in customers being unable to access their deposit and other accounts, or may jeopardize the viability of the operations of the individual banking organization or the stability of the financial sector.[4] The rule refers to these significant computer-security incidents as "notification incidents." The relevant agency receiving notice of notification incidents could assess the nature and severity of the incident, including whether it is isolated or widespread. The agency would then be in a position to take actions including, as appropriate, alerting other banking organizations and regulatory agencies, while protecting confidential supervisory information and facilitating requests for assistance. These actions could help to mitigate the impact of the incident, preserve the safe and sound operation of the banking organization, and reduce the risks to the financial sector.

This notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator and is not intended to include an assessment of the incident. The rule allows a banking organization to authorize or contract with a bank service provider to allow the bank service provider to make the relevant notifications to the banking organization's primary federal regulator on the banking organization's behalf. Moreover, a bank service provider as defined herein and in accordance with the Bank Service Company Act (BSCA)[5] is required to notify affected banking organization customers within four hours of when it experiences a computer-security incident that it reasonably believes could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours. "Bank service providers" would include both bank service companies and third-party service providers, under the BSCA.

2. Use of the information:

The notification requirement in the final rule is intended to serve as an early alert to a banking organization's primary federal regulator and is not intended to include an assessment of the incident. Additionally, a bank service provider as defined in the rule and in accordance with the Bank Service Company Act (BSCA)[6] is required to notify affected banking organization customers within four hours of when it experiences a computer-security incident that it reasonably believes could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

3. Consideration of the use of improved information technology:

Respondents may use any information technology that permits review by FDIC examiners.

4. Efforts to identify duplication:

Current reporting requirements do not sufficiently comprehend the risks posed by notification incidents. For example, under certain circumstances, a banking organization that has been a victim of a notification incident may have to file a Suspicious Activity

---

NIST, Computer Security Resource Center, *Glossary* (last accessed Sept. 20, 2020), *available at https://csrc.nist.gov/glossary/term/Dictionary*.

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

5 12 U.S.C. § 1861–67.

6 12 U.S.C. § 1861–67.

Report (SAR) to identify suspicious activity that might signal criminal actions (*e.g.*, money laundering or tax evasion). However, information from SARs, when available, may not cover all computer-security incidents impacting operations, and those incidents that are reported are often not reported timely enough for the agencies to take steps to reduce risks to the banking organization or the financial sector, if necessary. The rule is narrowly focused to address the need for timely alerts of notification incidents without interfering with or expanding other applicable reporting requirements.

5. Methods used to minimize burden if the collection has a significant impact on a substantial number of small entities:

This information collection would not have a significant impact on a substantial number of small entities.

6. Consequences to the Federal program if the collection were conducted less frequently:

Less frequent collection could result in incidents not being reported in a timely manner and could hinder the agencies' ability to take steps to reduce risks to banking organizations or to the financial sector.

7. Special circumstances necessitating collection inconsistent with 5 CFR Part 1320.5(d)(2):

There are no special circumstances. This information collection is conducted in accordance with the guidelines in 5 CFR 1320.5(d)(2).

8. Efforts to consult with persons outside the agency:

On January 12, 2021, the agencies published a notice of proposed rulemaking in the Federal Register (86 FR 2299) requesting comment on the information collection requirements contained in the proposed rule. The agencies received one Paperwork Reduction Act related comment which agreed that the proposed information collection has practical utility.

9. Payment or Gift to Respondents

None.

10. Any assurance of confidentiality:

Information will be kept private to the extent allowed by law.

11. Justification for questions of a sensitive nature:

No sensitive information is to be collected.

12. Estimate of hour burden including annualized hourly costs:

Summary of Annual Burden						
Information Collection Description	**Type of Burden**	**Obligation to Respond**	**Estimated Number of Respondents**	**Estimated Frequency of Responses**	**Estimated Time per Response (Hours)**	**Estimated Annual Burden (Hours)**
Notification Incident Reporting **12 CFR 304.23**	Recordkeeping	Mandatory	96	On Occasion	3	288
Service Provider Notification to Banking Organization **12 CFR 304.24**	Third Party Disclosure	Mandatory	802	On Occasion	3	2,406

Total Estimated Annual Burden **2,694 hours**

The rule establishes notification requirements for banking organizations upon the occurrence of a "computer security incident" that rises to the level of a "notification incident." A "notification incident" is defined as a "computer-security incident" that a banking organization reasonably believes could materially disrupt, degrade, or impair: (a) the ability of the banking organization 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; (b) any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or (c) those operations of a banking organization, 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.

A "computer-security incident" is defined as an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

The rule requires a banking organization to notify its primary federal banking regulator upon the occurrence of a "notification incident" at the banking organization. A banking organization may authorize or contract with a bank service provider to notify its primary federal banking regulator of such an incident on its behalf. The agencies recognize that the rule imposes a limited amount of burden, beyond what is usual and customary, on banking organizations in the event of a computer-security incident even if it does not rise to the level of a notification incident, as banking organizations will need to engage in an analysis to determine whether the relevant thresholds for notification are met. Therefore, the agencies' estimated burden per notification incident takes into account the burden

associated with such computer-security incidents.

The rule also requires a bank service provider, as defined in the rule, and in accordance with the BSCA, to notify affected banking organization customers within as soon as possible when it experiences a computer-security incident that it reasonably believes could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours. The agencies do not expect this requirement to impose third-party disclosure burden on bank service providers because such notifications to customers are common in the ordinary course of business.

Annualized Cost of Internal Hourly Burden:

The rule was co-authored with the Board and the OCC. In order to align the burdens across agencies, the FDIC uses the OCC's estimate of the cost of compensation equal to $115 per hour.[7] The FDIC believes the OCC estimate is a reasonable approximation of the foregone opportunity costs imposed by the rule.

FDIC estimates the total annual cost for the reporting and disclosure burden imposed by the rule by multiplying the total annual estimated burden hours (2,694) by the estimated Hourly Burden Cost ($115). The total estimated annual labor cost is estimated to be 2,694 hours * $115 / hour = $309,810.

13. Estimate of start-up costs to respondents:

None.

14. Estimate of annualized costs to the government:

None.

15. Analysis of change in burden:

This is a new information collection.

16. Information regarding collections whose results are planned to be published for statistical use:

No publication will be made of this information.

17. Display of expiration date:

Not applicable.

7 To estimate wages, the OCC reviewed May 2019 data for wages (by industry and occupation) from the U.S. Bureau of Labor Statistics (BLS) for credit intermediation and related activities excluding nondepository credit intermediaries (NAICS 5220A1). To estimate compensation costs associated with the rule, the OCC uses $115.19 per hour, which is based on the average of the 90th percentile for six occupations adjusted for inflation (3.1 percent as of Q1 2020 according to the BLS), plus an additional 33.4 percent for benefits (based on the percent of total compensation allocated to benefits as of Q4 2019 for NAICS 522: credit intermediation and related activities).

18. Exceptions to Certification

None.

B. Collection of Information Employing Statistical Methods

Not Applicable.