DEPARTMENT OF THE TREASURY
Office of the Comptroller of the Currency
12 CFR Part 53
[Docket ID OCC-2020-0038]
RIN 1557-AF02

FEDERAL RESERVE SYSTEM
12 CFR Part 225
Docket No. R- [•]
RIN 7100-AF [•]

FEDERAL DEPOSIT INSURANCE CORPORATION
12 CFR Part 304
RIN 3064-AF59

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

AGENCY: The Office of the Comptroller of the Currency, Treasury (OCC); the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC).

ACTION: Notice of proposed rulemaking.

SUMMARY: The OCC, Board, and FDIC (together, the agencies) invite comment on a notice of proposed rulemaking (proposed rule or proposal) that would require 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." The proposed rule would require such notification upon the occurrence of a notification incident as soon as possible and no later than 36 hours after the banking organization believes in good faith 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.

Moreover, a bank service provider would be required to notify at least two individuals at affected banking organization customers immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided for four or more hours.

DATES: Comments must be received by [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE ***FEDERAL REGISTER***].

ADDRESSES: You may submit comments, identified by RIN (1557-AF02 (OCC), 7100-AF (FRB), 3064-AF59 (FDIC)), by any of the following methods:

OCC:

Commenters are encouraged to submit comments through the Federal eRulemaking Portal, if possible. Please use the title "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" to facilitate the organization and distribution of the comments. You may submit comments by any of the following methods:

- **Federal eRulemaking Portal – Regulations.gov Classic or Regulations.gov Beta:**
    - **Regulations.gov Classic:** Go to *https://www.regulations.gov/*. Enter "Docket ID OCC-2020-0038" in the Search Box and click "Search." Click on "Comment Now" to submit public comments. For help with submitting effective comments please click on "View Commenter's Checklist." Click on the "Help" tab on the *Regulations.gov* home page to get information on using *Regulations.gov*, including instructions for submitting public comments.
    - **Regulations.gov Beta:** Go to *https://beta.regulations.gov/* or click "Visit New *Regulations.gov Site*" from the *Regulations.gov* Classic homepage. Enter

"Docket ID OCC-2020-0038" in the Search Box and click "Search." Public comments can be submitted via the "Comment" box below the displayed document information or by clicking on the document title and then clicking the "Comment" box on the top-left side of the screen. For help with submitting effective comments please click on "Commenter's Checklist." For assistance with the *Regulations.gov* Beta site, please call (877) 378-5457 (toll free) or (703) 454-9859 Monday-Friday, 9am-5pm ET or e-mail *regulations@erulemakinghelpdesk.com*.

- **Mail:** Chief Counsel's Office, Attention: Comment Processing, Office of the Comptroller of the Currency, 400 7th Street, SW, Suite 3E-218, Washington, DC 20219.
- **Hand Delivery/Courier:** 400 7th Street, SW, Suite 3E-218, Washington, DC 20219.

Instructions: You must include "OCC" as the agency name and "Docket ID OCC-2020-0038" in your comment. In general, the OCC will enter all comments received into the docket and publish the comments on the *Regulations.gov* website without change, including any business or personal information provided such as name and address information, e-mail addresses, or phone numbers. Comments received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. Do not include any information in your comment or supporting materials that you consider confidential or inappropriate for public disclosure.

Public Inspection: You may review comments and other related materials that pertain to this rulemaking action by any of the following methods:

- **Viewing Comments Electronically – Regulations.gov Classic or Regulations.gov Beta:**
    - **Regulations.gov Classic:** Go to *https://www.regulations.gov/*. Enter "Docket ID OCC-2020-0038" in the Search box and click "Search." Click on "Open Docket Folder" on the right side of the screen. Comments and supporting materials can be viewed and filtered by clicking on "View all documents and comments in this docket" and then using the filtering tools on the left side of the screen. Click on the "Help" tab on the *Regulations.gov* home page to get information on using *Regulations.gov*. The docket may be viewed after the close of the comment period in the same manner as during the comment period.
    - **Regulations.gov Beta:** Go to *https://beta.regulations.gov/* or click "Visit New *Regulations.gov Site*" from the *Regulations.gov* Classic homepage. Enter "Docket ID OCC-2020-0038" in the Search Box and click "Search." Click on the "Comments" tab. Comments can be viewed and filtered by clicking on the "Sort By" drop-down on the right side of the screen or the "Refine Results" options on the left side of the screen. Supporting materials can be viewed by clicking on the "Documents" tab and filtered by clicking on the "Sort By" drop-down on the right side of the screen or the "Refine Results" options on the left side of the screen." For assistance with the *Regulations.gov* Beta site, please call (877) 378-5457 (toll free) or (703) 454-9859 Monday-Friday, 9am-5pm ET or e-mail *regulations@erulemakinghelpdesk.com*. The docket may be viewed after the

close of the comment period in the same manner as during the comment period.

Board:

When submitting comments, please consider submitting your comments by e-mail or fax because paper mail in the Washington, DC area and at the Board may be subject to delay. You may submit comments, identified by Docket No. R- [·] RIN 7100-AF [·], by any of the following methods:

- **Agency Website**: *http://www.federalreserve.gov*. Follow the instructions for submitting comments at *http://www.federalreserve.gov/generalinfo/foia/RevisedRegs.cfm*.
- **E-mail**: *regs.comments@federalreserve.gov*. Include docket and RIN numbers in the subject line of the message.
- **FAX**: (202) 452-3819 or (202) 452-3102.
- **Mail**: Ann E. Misback, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW, Washington, DC 20551.

All public comments will be made available on the Board's website at: *http://www.federalreserve.gov/generalinfo/foia/RevisedRegs.cfm* as submitted, unless modified for technical reasons or to remove personally identifiable information at the commenter's request. Accordingly, comments will not be edited to remove any identifying or contact information. Public comments also may be viewed electronically or in paper in Room 3515, 1801 K Street NW (between 18th and 19th Streets NW), between 9:00 a.m. and 5:00 p.m. on weekdays.

FDIC:

- **Agency Website**: *https://www.fdic.gov/regulations/laws/federal/*. Follow the instructions for submitting comments on the Agency Website.
- **Email**: *Comments@fdic.gov*. Include RIN 3064-AF59 in the subject line of the message.
- **Mail**: James P. Sheesley, Assistant Executive Secretary, Attention: Comments, Federal Deposit Insurance Corporation, 550 17th Street, NW, Washington, DC 20429.
- **Hand Delivery/Courier**: Comments may be hand delivered to the guard station at the rear of the 550 17th Street, N.W., building (located on F Street) on business days between 7:00 a.m. and 5:00 p.m.

Public Inspection: All comments received will be posted without change to *https://www.fdic.gov/regulations/laws/federal/*—including any personal information provided— for public inspection. Paper copies of public comments may be ordered from the FDIC Public Information Center, 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226 by telephone at (877) 275-3342 or (703) 562-2200.

FOR FURTHER INFORMATION, CONTACT:

OCC: Patrick Kelly, Director, Critical Infrastructure Policy, (202) 649-5519, Jennifer Slagle Peck, Counsel, (202) 649-5490, or Priscilla Benner, Senior Attorney, Chief Counsel's Office, (202) 649-5490, or persons who are hearing impaired, TTY, (202) 649-5597, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219.

FRB: Nida Davis, Associate Director, (202) 872-4981, Julia Philipp, Lead Financial Institution Cybersecurity Policy Analyst, (202) 452-3940, Don Peterson, Supervisory Cybersecurity Analyst, (202) 973-5059, Systems and Operational Resiliency Policy, of the

Supervision and Regulation Division; Jay Schwarz, Special Counsel, (202) 452-2970, Claudia Von Pervieux, Senior Counsel (202) 452-2552, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets, NW, Washington, DC 20551. For the hearing impaired only, Telecommunications Device for the Deaf (TDD) users may contact (202) 263-4869.

FDIC: Robert C. Drozdowski, Special Assistant to the Deputy Director ((202) 898-3971), *RDrozdowski@FDIC.gov*, and Martin D. Henning, Deputy Director ((202) 898-3699), mhenning@fdic.gov, Division of Risk Management Supervision; Graham N. Rehrig, Senior Attorney ((703) 314-3401), *grehrig@fdic.gov*, and John Dorsey, Acting Supervisory Counsel ((202) 898-3807), *jdorsey@fdic.gov*, Legal Division, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20429.

SUPPLEMENTARY INFORMATION:

I. Introduction

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 malicious software to target weaknesses in the computers or networks of banking organizations supervised by the agencies.[2] Some cyberattacks 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 the ability of the banking organization to recover

[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*.

operations. The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), and the Federal Deposit Insurance Corporation (FDIC) (collectively, the agencies) are issuing a notice of proposed rulemaking (the proposal or proposed rule) that would require a banking organization to notify its primary federal regulator when the banking organization believes in good faith that a significant "computer-security incident" has occurred.[3] 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 agencies also recognize that a computer-security incident may be the result of non-malicious failure of hardware, software errors, actions of staff managing these computer resources, or potentially criminal in nature. Banking organizations that experience a computer-security incident that may be criminal in nature are expected to contact relevant law enforcement or security agencies, as appropriate, after the incident occurs.[4]

Moreover, banking organizations have become increasingly reliant on bank service providers to provide essential technology-related products and services. Service providers that provide services described in the Bank Service Company Act (BSCA)[5] to banking organizations (bank service providers)[6] also are vulnerable to cyber threats, which have the potential to disrupt, degrade, or impair the provision of banking services to their banking

[3] As defined by the proposed rule, a *computer-security incident* is an occurrence that results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that 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* NIST, Computer Security Resource Center, *Glossary* (last accessed Sept. 20, 2020), *available at https://csrc.nist.gov/glossary/term/Dictionary*.

[4] For example, a local FBI field office. *See* FBI, Contact Us, Field Offices, https://www.fbi.gov/contact-us/field-offices (last accessed Dec. 9, 2020).

[5] 12 U.S.C. 1861–67.

[6] Bank service providers would include both bank service companies and third-party providers under the BSCA.

organization customers. Therefore, the proposed rule would require a bank service provider to notify affected banking organization customers immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair the provision of services subject to the BSCA. Given the rule's purposes of ensuring that banking organizations provide timely notice of significant computer-security incident disruptions to the agencies, the agencies believe that bank service providers should contact at least two individuals at affected banking organizations to help ensure that notice has been received.

The agencies believe that it is important that the primary federal regulator of a banking organization be notified as soon as possible of a significant computer-security incident that could jeopardize the viability of the operations of an individual banking organization, result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector.[7] The proposed rule refers to these significant computer-security incidents as "notification incidents." Knowing about and responding to notification incidents affecting banking organizations is important to the agencies' missions for a variety of reasons, including the following:

- The receipt of notification-incident information may give the agencies earlier awareness of emerging threats to individual banking organizations and, potentially, to the broader financial system;
- An incident may so severely impact a banking organization that it can no longer support its customers, and the incident could impact the safety and

[7] 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.

soundness of the banking organization, leading to its failure. In these cases, the sooner the agencies know of the event, the better they can assess the extent of the threat and take appropriate action;

- Based on the agencies' broad supervisory experiences, they may be able to provide information to a banking organization that may not have previously faced a particular type of notification incident;
- The agencies would be better able to conduct analyses across supervised banking organizations to improve guidance, adjust supervisory programs, and provide information to the industry to help banking organizations protect themselves; and
- Receiving notice would enable the primary federal regulator to facilitate and approve requests from banking organizations for assistance through the U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP).[8]

As discussed below, current reporting requirements related to cyber incidents are neither designed nor intended to provide timely information to regulators regarding such incidents.

II. Review of Existing Regulations and Guidance

The agencies considered whether the information that would be provided under the

[8] 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* (Oct. 2018) identifies additional information available to banking organizations. *Available at https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf* (last accessed Nov. 29, 2020).

proposed rule could be obtained through existing reporting standards. Currently, banking organizations may be required to report certain instances of disruptive cyber-events and cyber-crimes through the filing of Suspicious Activity Reports (SARs), and they are generally expected to notify their primary federal regulator "as soon as possible" when they become "aware of an incident involving unauthorized access to or use of sensitive customer information."[9] These reporting standards provide the agencies with valuable insight regarding cyber-related events and information-security compromises; however, these existing requirements do not provide the agencies with sufficiently timely information about every notification incident that would be captured by the proposed rule.

Under the reporting requirements of the Bank Secrecy Act (BSA) and its implementing regulations, certain banking organizations are required to file SARs when they detect a known or suspected criminal violation of federal law or a suspicious transaction related to a money-laundering activity.[10] While the agencies monitor SARs regularly, SARs serve a different purpose from this proposed incident notification requirement and do not require reporting of every incident captured by the proposed definition of a notification incident. Moreover, the 30-calendar-day reporting requirement under the BSA framework (with an additional 30 calendar days provided in certain circumstances) does not provide the agencies with sufficiently timely notice of reported incidents.

Additionally, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, which interprets section 501(b) of the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines Establishing Information

[9] *See* 12 CFR pt. 30, app'x B, supp. A (OCC); 12 CFR pt. 208, app'x D-2, supp. A, 12 CFR 211.5(l), 12 CFR pt. 225, app'x. F, supp. A (Board); 12 CFR pt. 364, app'x B, supp. A (FDIC) (italics omitted).
[10] *See, e.g.,* 31 U.S.C. 5311 *et seq.*; 31 CFR subtit. B, ch. X.

Security Standards, generally sets forth the supervisory expectation that a banking organization notify its primary federal regulator "as soon as possible" if the organization becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information.[11] While this may provide the agencies with notice of certain computer-security incidents, this standard is too narrow in scope to address all relevant computer-security incidents that would be covered by the proposed rule. In particular, the GLBA notification standard focuses on incidents that result in the compromise of sensitive customer information and, therefore, does not include the reporting of incidents that disrupt operations but do not compromise sensitive customer information.

Finally, the BSCA requires a banking organization to notify the appropriate Federal banking agency of the existence of service relationships within thirty days after the making of such service contracts or the performance of the service, whichever occurs first.[12] However, the BSCA has no notification requirements if the service is disrupted.

III. The Proposal

The proposed rule would establish two primary requirements, which would promote the safety and soundness of banking organizations and be consistent with the agencies' authorities to supervise these entities.[13] First, the proposed rule would require a banking organization to notify the agencies of a notification incident. In particular, a banking organization would be required to notify its primary federal regulator of any computer-security incident that rises to the level of a notification incident as soon as possible and no

[11] *See* 15 U.S.C. 6801; 12 CFR pt. 30, app'x B, supp. A (OCC); 12 CFR pt. 208, app'x D-2, supp. A, 12 CFR 211.5(l), 12 CFR pt. 225, app'x. F, supp. A (Board); 12 CFR pt. 364, app'x B, supp. A (FDIC).
[12] 12 U.S.C. 1867(c)(2).
[13] *See* 12 U.S.C. 1, 93a, 161, 481, 1463, 1464, 1861–1867, and 3102 (OCC); 12 U.S.C. 321–338a, 1467a(g), 1818(b), 1844(b), 1861–1867, 3101 *et seq.*, and 5365 (Board); 12 U.S.C. 1463, 1811, 1813, 1817, 1819, and 1861–1867 (FDIC).

later than 36 hours after the banking organization believes in good faith that a notification incident has occurred. The agencies do not expect that a banking organization would typically be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident. Rather, the agencies anticipate that a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident. In this context, the agencies recognize banking organizations may not come to a good faith belief that a notification incident has occurred outside of normal business hours. Only once the banking organization has made such a determination would the requirement to report within 36 hours begin.

The proposed rule would define a *computer-security incident* as an occurrence that (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The proposed rule would define a *notification incident* as a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair—

> 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;
>
> 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
>
> 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.

Second, the proposed rule would require a bank service provider of a service described under the BSCA to notify at least two individuals at affected banking organization customers immediately after experiencing a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours. As technological developments have increased in pace, banks have become increasingly reliant on bank service providers to provide essential technology-related products and services. The impact of computer-security incidents at bank service providers can flow through to their banking organization customers. Therefore, in order for a banking organization to be able to provide relevant notifications to its primary federal regulator in a timely manner, it needs to receive prompt notification of computer-security incidents from its service providers.

Bank services that are subject to the BSCA include "check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution," as well as components that underlie these activities.[14] Other services that are subject to the BSCA include data processing, back office services, and activities related to credit extensions, as well as components that underlie these activities.[15]

---

[14] *See* 12 U.S.C. 1863–64.

[15] *See* 12 U.S.C. 1864(f). Under the BSCA, such services must be permissible for bank holding companies under section 4(c)(8) of the Bank Holding Company Act of 1956, as amended, and section 225.28 of the Board's Regulation Y. 12 U.S.C. 1841 *et seq.*; 12 CFR 225.28. Activities permissible under section 225.28 are: (1) extending credit and servicing loans; (2) activities related to extending credit; (3) leasing personal or real property; (4) operating nonbank depository institutions; (5) trust company functions; (6) financial and

The proposed rule would apply to the following banking organizations:

For the **OCC**, "banking organizations" would include national banks, federal savings associations, and federal branches and agencies.

For the **Board**, "banking organizations" would include all U.S. bank holding companies and savings and loan holding companies; state member banks; the U.S. operations of foreign banking organizations; Edge and agreement corporations.

For the **FDIC**, "banking organizations" would include all insured state nonmember banks, insured state-licensed branches of foreign banks, and state savings associations.

To clarify, not all "computer-security incidents" require a banking organization to notify its primary federal regulator; only those that rise to the level of "notification incidents" require notification. Other computer-security incidents, such as a limited distributed denial of service attack that is promptly and successfully managed by a banking organization, would not require notice to the appropriate agency.

The following is a non-exhaustive list of events that would be considered "notification incidents" under the proposed rule:

1. Large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (e.g., more than 4 hours);
2. A bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and recovery time is undeterminable;

investment advisory activities; (7) agency transactional services for customer investments; (8) investment transactions as principal; (9) management consulting and counseling activities; (10) support services; (11) insurance agency and underwriting; (12) community development activities; (13) money orders, savings bonds, and traveler's checks; and (14) data processing. 12 CFR 225.28.

3. A failed system upgrade or change that results in widespread user outages for customers and bank employees;

4. An unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan;

5. A computer hacking incident that disables banking operations for an extended period of time;

6. Malware propagating on a banking organization's network that requires the banking organization to disengage all Internet-based network connections; and

7. A ransom malware attack that encrypts a core banking system or backup data.

The agencies expect that banking organizations would consider whether other significant computer-security incidents they experience, beyond those listed above, constitute notification incidents for purposes of notifying the appropriate agency.

The definition of "notification incident" includes language that is consistent with the "core business line" and "critical operation" definitions included in the resolution-planning rule issued by the Board and FDIC under section 165(d) of the Dodd-Frank Act.[16] In particular, the second prong of the notification incident definition identifies incidents that would impact core business lines, and the third prong identifies incidents that would impact critical operations. Banking organizations subject to the Resolution Planning Rule can use the core business lines and critical operations identified in their resolution plans[17] to identify incidents that should be reported under the second and third prongs of the proposed rule.

[16] Section 165(d) of the Dodd-Frank Act and the resolution-plan rule, 12 CFR parts 363 and 381 (the Resolution Planning Rule), require certain financial companies to report periodically to the FDIC and FRB their plans for rapid and orderly resolution in the event of material financial distress or failure. On November 1, 2019, the FDIC and FRB published in the *Federal Register* amendments to the Resolution Planning Rule. *See* 84 FR 59194.

[17] Elements of both the "core business lines" and "critical operations" definitions from the Resolution Planning

The agencies do not expect banking organizations that are not subject to the Resolution Planning Rule to identify "core business lines" or "critical operations," or to develop procedures to determine whether they engage in any operations, the failure or discontinuance of which would pose a threat to the financial stability of the United States. However, the agencies do expect all banking organizations to have a sufficient understanding of their lines of business to be able to notify the appropriate agency of notification incidents that could result in a material loss of revenue, profit, or franchise value to the banking organization.

If a banking organization is a subsidiary of another banking organization that is also subject to the notification requirements of this proposed rule, the agencies expect the subsidiary banking organization to alert its parent banking organization as soon as possible of the notification incident, in addition to notifying its primary federal regulator. The parent banking organization would need to make a separate assessment of whether it, too, has suffered a notification incident about which it must notify its primary federal regulator. An entity that is not itself a banking organization, but that is a subsidiary of a banking organization, would not have its own separate notification requirement under this proposed rule. Instead, if a computer-security incident were to occur at a non-bank subsidiary of a banking organization, the parent banking organization would be expected to assess whether the incident was a notification incident, and if so, it would be required to notify its primary federal regulator.

Rule are incorporated in the proposed "notification incident" definition. Under the Resolution Planning Rule, "core business lines" means those business lines of the covered company, including associated operations, services, functions and support, that, in the view of the covered company, upon failure would result in a material loss of revenue, profit, or franchise value, and "critical operations" means those operations of the covered company, including associated services, functions, and support, the failure or discontinuance of which would pose a threat to the financial stability of the United States. *See* 12 CFR 363.2, 381.2.

The proposed notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator about a notification incident and is not intended to include an assessment of the incident. As such, no specific information is required for the notice, and the proposed rule does not include any prescribed reporting forms or templates to minimize reporting burden. The agencies believe that in most cases banking organizations would eventually notify their primary regulator when an event occurs that meets the high threshold of a notification incident and that this proposed rule is formalizing a process that the agencies' experience suggest already exists. The agencies recognize that a banking organization may be working expeditiously to resolve the notification incident—either directly or through a bank service provider—at the time it would be expected to notify its primary federal regulator. The agencies believe, however, that 36 hours is a reasonable amount of time after a banking organization believes in good faith that a notification incident has occurred to notify its primary federal regulator, particularly because the notice would not need to include an assessment of the incident. The agencies expect only that banking organizations share general information about what is known at the time. Moreover, the notice could be provided through any form of written or oral communication, including through any technological means (e.g., email or telephone), to a designated point of contact identified by the banking organization's primary federal regulator (e.g., an examiner-in-charge, local supervisory office, or a cyber-incident operations center). The notification, and any information provided by a banking organization related to the incident, would be subject to the agencies' confidentiality rules.

Under the proposed rule, a bank service provider would be required to notify at least two individuals at affected banking organization customers immediately after it experiences a

computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours. A bank service provider would not be expected to assess whether the incident rises to the level of a notification incident for a banking organization customer. The banking organization would be responsible for making that determination because a bank service provider may not know if the services provided are critical to the banking organization's operations. If, after receiving such notice from a bank service provider, the banking organization determines that a notification incident has occurred, the banking organization would be required to notify its primary federal regulator in accordance with this proposed rule. Typically, existing bank service provider agreements that support operations that are critical to a banking organization customer require notification to the customer as soon as possible in the event of a material incident during the normal course of business, and the agencies believe that the procedures in place to do so will generally include some redundancy to ensure that notification occurs.

Under the proposal, the agencies would expect bank service providers to continue to provide a banking organization customer with prompt notification of these material incidents. The agencies believe that it is practical for a bank service provider to immediately notify at least two individuals at their affected banking organization customers after experiencing a computer-security incident of the severity described in the proposed rule because the notice would not need to include an assessment of the incident, and the agencies observe that there are effective automated systems for doing so currently. The agencies expect only that bank service providers would make a best effort to share general information about what is known at the time. Regulators would enforce the bank service provider notification requirement directly against bank service providers and would not cite a banking

organization because a service provider fails to comply with the service provider notification requirement.

This proposal is not expected to add significant burden on banking organizations. Banking organizations should already have internal policies for responding to computer-security incidents, which the agencies believe generally already include processes for notifying their primary federal regulator and other stakeholders of incidents within the scope of the proposal. However, these processes are not uniform or consistent between institutions and have not always resulted in timely notification being provided to the applicable regulator, which is why the agencies are issuing this proposal. This proposal also is not expected to add significant burden on bank service providers. The agencies' experiences with conducting bank service provider contract reviews during examinations indicates that most of these contracts include incident-reporting provisions. As a result, this proposal is not expected to add significant burden on a material number of bank service providers.

Each agency may provide additional clarification and guidance to its supervised banking organizations on how best to communicate with the agencies to implement the notification requirements of the rule.

IV. Impact Analysis

Covered banking organizations under the proposed rule would include all depository institutions, holding companies, and certain other financial entities that are supervised by one of the agencies. According to recent Call Report and other data, the agencies supervise approximately 5,000 depository institutions along with a number of holding companies and other financial services entities that would be covered under the proposed rule.[18]

[18] September 30, 2020 Call Report Data.

In addition, the proposed rule would require bank service providers as described in the BSCA to notify at least two individuals at affected banking organization customers immediately after the bank service providers experience a computer-security incident that they believe in good faith could disrupt, degrade, or impair services they provide subject to the BSCA for 4 or more hours. This requirement would enable a banking organization to promptly respond to an incident, determine whether it must notify its primary federal regulator that a notification incident has occurred, and take other appropriate measures related to the incident. The agencies do not have data on the number of bank service providers that would be affected by this requirement. However, several known bank service providers have self-selected the North American Industry Classification System (NAICS) industry "Computer System Design and Related Services" (NAICS industry code 5415) as their primary business activity. As a conservative estimate of the population of covered bank service providers for this analysis, the agencies assume that all firms in this industry are bank service providers.[19] According to Census counts, there were 120,220 firms in the United States under NAICS code 5415 in 2017, the most recent year for which such data is available.[20]

Benefits

The agencies believe that prompt notification of these incidents would provide the following benefits to banking organizations and the financial industry as a whole.

Notification may assist the relevant agencies in determining whether the incident is

[19] NAICS code 5415 most likely contains many firms that are not bank service providers, so the agencies believe using the population of firms in this industry is an overestimate. However, there may be some bank service providers that do not self-identify under NAICS code 5415.
[20] *See* U.S. Census Bureau, 2017 SUSB Annual Data Tables by Establishment Industry (Mar. 2020), https://www.census.gov/data/tables/2017/econ/susb/2017-susb-annual.html.

isolated or is one of many simultaneous identical or similar incidents at multiple banking organizations. If the notification incident is isolated to a single banking organization, the primary federal regulator may be able to facilitate requests for assistance to the affected organization, arranged by the U.S. Treasury OCCIP, to minimize the impact of the incident. This benefit may be greatest for small banking organizations with more limited computer security resources. If the notification incident is one of many simultaneous identical or similar incidents at multiple banking organizations, the agencies may also alert other banking organizations of the threat, as appropriate, while protecting confidential supervisory information, recommend preventative measures in order to better manage or prevent reoccurrence of similar incidents, or otherwise help coordinate the response and mitigation efforts. Receiving notification incident information from multiple banking organizations would also allow regulators to conduct analyses across entities to improve guidance, to adjust supervisory programs to limit the reoccurrence of such incidents in the future, and to provide information to the industry to help banking organizations protect themselves against future computer-security incidents.

The proposal may help reduce losses in the event a notification incident is so significant that it jeopardizes a banking organization's viability, as the proposal will provide additional time for the agencies to prepare to handle a potential failure as cost-effectively and non-disruptively as possible.

The agencies do not have the information to quantify the potential benefits of the proposed rule because the benefits depend on the breadth and severity of future notification incidents, the specifics of those incidents, and the value of the assistance approved by the agencies, among other things. In addition, the agencies believe that the proposed rule would

formalize a process that already exists, based on the agencies' experiences. Nevertheless, as previously discussed, banking organizations face a heightened risk of disruptive and destructive attacks that have increased in frequency and severity in recent years; therefore, the agencies believe that the benefits of the proposed rule would exceed the costs—detailed below.

Costs

The proposed rule would require banking organizations to notify their primary federal regulator as soon as possible and no later than 36 hours after a banking organization has determined that a notification incident has occurred. The agencies reviewed available supervisory data and SARs involving cyber events against banking organizations to develop an estimate of the number of notification incidents expected to be reported annually. This review focused 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 may occur on an annual basis.[21] The agencies specifically invite comment on the estimated number of incidents.

The agencies estimate that, upon occurrence of a notification incident, the affected banking organization may incur up to three hours of staff time to coordinate internal communications, consult with its bank service provider, if appropriate, and notify the banking organization's primary federal regulator. This may include discussion of the incident among staff of the banking organization, such as the Chief Information Officer,

[21] The agencies used conservative judgment when assessing whether a cyber-event might have risen to the level of a notification incident, so the approach may overestimate the number. However, the approach may also underestimate the number of notification incidents since supervisory and SAR data may not capture all such incidents.

Chief Information Security Officer, a senior legal or compliance officer, and staff of a bank service provider, as appropriate, and liaison with senior management of the banking organization. The agencies believe that the regulatory burden associated with the notice requirement would be *de minimis*, because the communications that led to the determination of the notification incident would occur regardless of the proposed rule.[22]

The proposed rule also requires a bank service provider, as defined herein and in accordance with the BSCA, to notify at least two individuals at affected banking organization customers immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours. The agencies do not have data on the frequency of incidents that would require bank service providers to notify their customers who are banking organizations. For purposes of this proposed rule, the agencies assume that 36 bank service providers, or 2%[23] of the 120,220 firms under NAICS code 5415, could experience a computer-security incident each year that would require notification to affected banking organization customers. The agencies specifically invite comment on the estimated number of incidents.

The agencies believe that bank service providers would have automated systems allowing them to identify banking organization customers when a computer-security incident that meets the criteria for notification has occurred and for contacting at least two individuals at affected banking organization customers. Furthermore, the agencies anticipate that such firms would need approximately one hour to determine that a computer-security incident

[22] Even at an elevated labor compensation rate of $200 per hour, the proposed rule would only impose additional compliance costs of $600 per notification.

[23] This is consistent with the estimate of the percentage of banking organizations that have notification incidents.

meets the notification criteria and two hours to identify the customers affected by the service disruption and provide notification that an incident has occurred. These activities would total 7,213 hours per year for the population of bank service providers described above.[24] The agencies believe that the additional compliance costs would be *de minimis* for each affected bank service provider.[25] Post-notification activities such as providing technical support to affected bank organization customers that would be provided during the normal course of business when managing and resolving a computer security incident are beyond the scope of the notification requirement.

The agencies invite comments on these expected benefits and costs.

V. Alternatives Considered

The agencies considered several alternatives to the proposal. The agencies considered leaving the current regulations unchanged. The agencies rejected this alternative because of the significant risks that notification incidents pose to banking organizations and to the financial sector.

The agencies considered limiting the definition of notification incidents to those covered by the SAR-filing requirements. In this alternative, submission of a SAR would have served as notification of such an incident. This approach would have eliminated the additional compliance burden but would have delayed the notification and decreased the benefits provided by the proposed rule. In the proposal, however, the agencies determined that, to minimize regulatory burden, the notice requirement would not include the level of detail required of a SAR (which could otherwise have created a significant burden to

[24] 7,213 hours = 120,220 firms * 2% per year frequency of incident * 3 hours per incident.
[25] Even at an elevated labor compensation rate of $200 per hour, the proposed rule would only impose additional compliance costs of $600 per notification.

complete as a banking organization manages a notification incident).

The agencies considered expanding the definition of notification incident to include any incident that might disrupt a banking organization's systems or any unauthorized access to the banking organization's sensitive customer data. However, the agencies ultimately sought to strike a balance that would minimize compliance burden by focusing only on events that are likely to cause significant harm to banking organizations.

VI. Request for Comments

The agencies seek comment on all aspects of their proposal and more specifically on the following:

1. How should the definition of "computer-security incident" be modified, if at all? For example, should it include only occurrences that result in actual harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits? Should it include only occurrences that constitute an actual violation of security policies, security procedures, or acceptable use policies?
2. How should the definition of "notification incident" be modified, if at all? For example, instead of "computer-security incident," should the definition of "notification incident" refer to other NIST terms and definitions, or another recognized source of terms and definitions? Should the standard for materially disrupt, degrade, or impair be altered to reduce potential redundancy between the terms or to consider different types of impact on the banking organization? Should the definition not include language that is consistent with the "core business line" and "critical operation" definitions included in the resolution-

planning rule? Should those elements of the definition only apply to banking organizations that have resolution planning requirements?

3. How should the 36 hour timeframe for notification be modified, if at all, and why? Should it be made shorter or longer? Should it start at a different time? Should the timeframe be modified for certain types of notification incidents or banking organizations (for example, should banks with total assets of less than $10 billion have a different timeframe)?

4. Is the proposed requirement that banking organizations and bank service providers notify the appropriate party when they "believe in good faith" that they are experiencing or have experienced a notification incident or computer-security incident, as applicable, sufficiently clear such that banking organizations and bank service providers understand when they should provide notice? How should the "believes in good faith" standard be modified, if at all? For example, should the standard be "reasonably believes" for either banking organizations or bank service providers?

5. How should notification by banking organizations under the proposed rule be provided to the agencies? Should the agencies adopt a process for joint notification to the agencies in cases where multiple affiliates of a banking organization have notification requirements to different agencies? If so, how should joint notification be done and why? Should the agencies adopt centralized points of contact to receive notifications or should notifications be provided to regional offices (such as Federal Reserve Banks) or banking organization-specific supervisory teams?

6. The proposed rule's definition of "banking organizations" and "bank service providers" would include the financial market utilities (FMUs) that are chartered as a State member bank or Edge corporation, or perform services subject to regulation and examination under the BSCA. Are there unique factors that the agencies should consider in determining how notification requirements should apply to these FMUs? For designated FMUs for which the Board is the Supervisory Agency under Title VIII of the Dodd-Frank Act, would notification requirements best be conveyed through this proposed rule or through amendments to the Board's Regulation HH?

7. What other types of entities regulated by the agencies should be added to the rule as "banking organizations" that would be subject to the rule? Why?

8. Which entities proposed in the rule as "banking organizations" should be removed from the rule? Why?

9. Do existing contracts between banking organizations and bank service providers already have provisions that would allow banking organizations to meet the proposed notification incident requirements?

10. Does the definition of "bank service provider" in the proposed rule appropriately capture the services about which banking organizations should be informed in the event of disruptions? Should all the services included in the Bank Service Company Act be included for purposes of banking organizations receiving notice of disruptions from their bank service providers? If not, which services should require a bank service provider to notify its affected banking organization customers when those services are disrupted, and why? Should the requirement

only attach to a subset of services provided to banking organizations under the BSCA or should it only attach to certain bank service providers, such as those that are examined by the federal banking agencies?

11. Should the proposed rule for bank service providers require bank service providers to notify all banking organization customers or only those affected by a computer-security incident under the proposed rule?

12. Within what timeframe should bank service providers provide notification to banking organizations? Is immediate notification after experiencing a disruption in services provided to affected banking organization customers and to report to those organizations reasonable? If not, what is the appropriate amount of time for a bank service provider to determine it has experienced a material disruption in service that impacts its banking organization customers, and why?

13. The agencies understand that many existing contracts between banking organizations and bank service providers contain notification provisions regarding material incidents and that, generally, bank service providers use automated systems to notify banking organizations of service disruptions. The agencies are seeking information on how bank service providers currently notify banking organizations of service disruptions under existing contracts between bank service providers and banking organizations. Do those contracts contemplate the provision of notice to at least two individuals at an affected banking organization? Is the method of notice specified in existing contracts (for example, email, telephone, etc.) sufficient to allow bank service providers to provide notice of computer-security incidents to at least two individuals at affected banking

organizations? If not, how best could the requirement for bank service providers to notify at least two individuals at affected banking organizations be achieved most efficiently and cost effectively for both parties?

14. Describe circumstances in which a bank service provider would become aware of a material disruption that could be a notification incident for banking organization customers but the banking organization customers would not be aware of the incident. Would it be overly burdensome to certain bank service providers, such as smaller bank service providers, to provide notice of material disruptions, degradations, or impairments to their affected banking organization customers and, if so, why?

15. The agencies invite comments on specific examples of computer-security incidents that should, or should not, constitute notification incidents.

16. The agencies invite comments on the methodology used to estimate the number of notification incidents per year that would need to be reported under the proposed rule.

Written comments must be received by the agencies no later than [insert date 90 days after publication in the *Federal Register*].

VII. Regulatory Analysis and Procedure

Paperwork Reduction Act

Certain provisions of the proposed rule contain "collection of information" requirements within the meaning of the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3501–3521). In accordance with the requirements of the PRA, the agencies may not conduct or sponsor, and the respondent is not required to respond to, an information collection unless

it displays a currently valid Office of Management and Budget (OMB) control number. The agencies will request new control numbers for this information collection. The information collection requirements contained in this joint notice of proposed rulemaking have been submitted to OMB for review and approval by the OCC and FDIC under section 3507(d) of the PRA (44 U.S.C. 3507(d)) and section 1320.11 of OMB's implementing regulations (5 CFR part 1320). The Board reviewed the proposed rule under the authority delegated to the Board by OMB.

The proposed rule contains a reporting requirement that is subject to the PRA. The reporting requirement is found in sections 53.3 (OCC), 225.302 (FRB), and 304.23 (FDIC) of the proposed rule, which require a banking organization to notify its primary federal bank regulatory agency of the occurrence of a "notification incident" at the banking organization.

The proposed rule also contains a disclosure requirement that is subject to the PRA. The disclosure requirement is found in sections 53.4 (OCC), 225.303 (FRB), and 304.24 (FDIC) of the proposed rule, which require a bank service provider to notify at least two individuals at affected banking organization customers immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

Comments are invited on:

(a) whether the collections of information are necessary for the proper performance of the agencies' functions, including whether the information has practical utility;

(b) the accuracy of the estimates of the burden of the information collections, including the validity of the methodology and assumptions used;

(c) ways to enhance the quality, utility, and clarity of the information to be collected;

(d) ways to minimize the burden of the information collections on respondents, including through the use of automated collection techniques or other forms of information technology; and

(e) estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information. All comments will become a matter of public record.

Comments on aspects of this notice that may affect reporting requirements and burden estimates should be sent to the addresses listed in the ADDRESSES section of this Supplementary Information. A copy of the comments may also be submitted to the OMB desk officer for the Agencies: By mail to U.S. Office of Management and Budget, 725 17th Street NW, #10235, Washington, DC 20503 or by facsimile to (202) 395-5806, Attention, Federal Banking Agency Desk Officer.

Proposed Information Collection

Title of Information Collection: Computer-Security Incident Notification.

Frequency of Response: On occasion; event-generated.[26]

Affected Public: Businesses or other for-profit.

Respondents:

OCC: National banks, federal savings associations, federal branches and agencies, and bank service providers.

FDIC: All insured state nonmember banks, insured state-licensed branches of foreign banks, State savings associations, and bank service providers.

Board: All state member banks (as defined in 12 CFR 208.2(g)), bank holding companies (as

[26] For purposes of these calculations, the agencies assume that the frequency is 1 response per respondent.

defined in 12 U.S.C. 1841), savings and loan holding companies (as defined in 12 U.S.C. 1467a), foreign banking organizations (as defined in 12 CFR 211.21(o)), foreign banks that do not operate an insured branch, state branch or state agency of a foreign bank (as defined in 12 U.S.C. 3101(b)(11) and (12)), Edge or agreement corporations (as defined in 12 CFR 211.1(c)(2) and (3)), and bank service providers.

Number of Respondents:[27]

OCC: Reporting – 22; Disclosure – 801.

FDIC: Reporting – 96; Disclosure – 802.

Board: Reporting – 32; Disclosure – 801.

Estimated Hours per Response:

Reporting – Sections 53.3 (OCC), 225.302 (FRB), and 304.23 (FDIC): 3 hours.

Disclosure – Sections 53.4 (OCC), 225.303 (FRB), and 304.24 (FDIC): 3 hours.

Estimated Total Annual Burden:

OCC: Reporting –66 hours; Disclosure – 2,403 hours.

FDIC: Reporting –288 hours; Disclosure – 2,406 hours.

Board: Reporting –96 hours; Disclosure – 2,403 hours.

Abstract: The proposed rule would establish 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

[27] 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. The number of respondents for the disclosure requirement is based on an assumption of a 2% per year frequency of incidents from 120,220 firms, which is divided equally among the OCC, FDIC, and Board.

organization believes in good faith could materially disrupt, degrade, or impair:

- 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;
- 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
- 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 harm to the confidentiality, integrity, or availability of an information system or the information that 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 proposed rule would require a banking organization to notify its primary federal banking regulator upon the occurrence of a "notification incident" at the banking organization. The agencies recognize that the proposed rule would impose 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 proposed rule also would require a bank service provider, as defined herein and in accordance with the BSCA, to notify at least two individuals at affected banking organization customers immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours.

Regulatory Flexibility Act

OCC: The Regulatory Flexibility Act (RFA), 5 U.S.C. 601 *et seq.*, requires an agency, in connection with a proposed rule, to prepare an Initial Regulatory Flexibility Analysis describing the impact of the rule on small entities (defined by the Small Business Administration (SBA) for purposes of the RFA to include commercial banks and savings institutions with total assets of $600 million or less and trust companies with total assets of $41.5 million or less) or to certify that the proposed rule would not have a significant economic impact on a substantial number of small entities. The OCC currently supervises approximately 745 small entities.

Because the proposed rule impacts all OCC-supervised institutions, as well as all bank service providers, it would impact a substantial number of small entities. However, the expected costs of the proposal would be *de minimis*. Many banks already have internal policies for responding to security incidents, which include processes for notifying their primary regulator and other stakeholders of incidents within the scope of the proposal. Additionally, while the OCC believes bank service provider contracts may already include these provisions, if current contracts do not include these provisions, then the OCC does not expect the implementation of these provisions to impose a material burden on bank service

providers. Therefore, the OCC certifies that the proposed rule, if implemented, would not have a significant economic impact on a substantial number of small entities.

Board: The Board has considered the potential impact of the proposed rule on small entities in accordance with section 603 of the RFA.[28] Based on the Board's analysis, and for the reasons stated below, the Board believes that this proposed rule will not have a significant economic impact on a substantial of number of small entities.

As discussed in the **Supplementary Information**, the agencies are proposing to require a banking organization to notify its primary federal regulator as soon as possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred. The proposed rule would establish a significant computer-security incident notification requirement, which would support the safety and soundness of entities supervised by the agencies. The proposed rule also would require a bank service provider, as defined herein and in accordance with the BSCA, to notify at least two individuals at affected banking organization customers immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair the provision of services subject to the BSCA for four or more hours.

The Board's rule applies to state-chartered banks that are members of the Federal Reserve System, bank holding companies, savings and loan holding companies, U.S. operations of foreign banking organizations, Edge and agreement corporations (collectively, "Board-regulated entities"). As described in the Impact Analysis section, requirements under the proposed rule would apply to all Board-regulated entities. Under regulations issued by the Small Business Administration, a small entity includes a depository institution, bank

[28] 5 U.S.C. 603.

holding company, or savings and loan holding company with total assets of $600 million or less and trust companies with total receipts of $41.5 million or less.[29] According to Call Reports and other Board reports, there were approximately 472 state member banks, 2,925 bank holding companies, 132 savings and loan holding companies, and 16 Edge and agreement corporations that are small entities.[30] In addition, the proposed rule affects all bank service providers that provide services subject to the BSCA.[31] The Board is 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.

The proposed rule would require all banking organizations to notify their primary federal regulator as soon as possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred. The agencies estimate that, upon occurrence of a notification incident, an affected banking organization may incur compliance costs of up to three hours of staff time to coordinate internal communications, consult with its bank service provider, if appropriate, and notify the banking organization's primary federal regulator. As described in the Impact Analysis section above, this requirement is estimated to affect a relatively small number of Board-regulated entities. The agencies believe that any compliance costs associated with the notice requirement would be *de minimis*, because the communications that led to the determination of the notification incident would have occurred regardless of the proposed rule.

[29] *See* 13 CFR 121.201; 84 FR 34261 (July 18, 2019).
[30] State member bank data is derived from March 31, 2020 Call Reports. Data for bank holding companies and savings and loan holding companies are derived from the June 30, 2020, FR Y-9C and FR Y-9SP. Data for Edge and agreement corporations are derived from the December 31, 2019 and March 31, 2020, FR-2086b.
[31] Discussed in detail in the Impact Analysis section.

The proposed rule also would require a bank service provider, as defined herein and in accordance with the BSCA, to notify at least two individuals at affected banking organization customers immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair the provision of services subject to the BSCA for four or more hours. As described in the Impact Analysis section above, the agencies believe that any compliance costs associated with the implementation of this requirement would be *de minimis* for each affected bank service provider. There are no other recordkeeping, reporting or compliance requirements associated with the proposed rule.

The Board has not identified any federal statutes or regulations that would duplicate, overlap, or conflict with the proposed revisions, and the Board is not aware of any significant alternatives to the final rule that would reduce the economic impact on Board-regulated small entities. For the reasons stated above, the Board believes that this proposed rule will not have a significant economic impact on a substantial number of small entities. The Board welcomes comment on all aspects of its analysis. In particular, the Board requests that commenters describe the nature of any impact on small entities and provide empirical data to illustrate and support the extent of the impact.

FDIC: The Regulatory Flexibility Act (RFA) generally requires an agency, in connection with a proposed rule, to prepare and make available for public comment an initial regulatory flexibility analysis that describes the impact of a proposed rule on small entities.[32] However, a regulatory flexibility analysis is not required if the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities. The Small Business Administration (SBA) has defined "small entities" to include banking

[32] 5 U.S.C. 601 *et seq.*

organizations with total assets of less than or equal to $600 million.[33] Generally, the FDIC considers a significant effect to be a quantified effect in excess of 5 percent of total annual salaries and benefits per institution, or 2.5 percent of total noninterest expenses. The FDIC believes that effects in excess of these thresholds typically represent significant effects for FDIC-supervised institutions. For the reasons described below, the FDIC certifies that the proposed rule will not have a significant economic impact on a substantial number of small entities.

As described in the Impact Analysis section, the proposed rule is expected to affect all institutions supervised by the FDIC. According to the most recent Call Reports, the FDIC supervises 3,270 insured depository institutions (FDIC-supervised IDIs).[34] Of these, approximately 2,492 FDIC-supervised IDIs would be considered small entities for the purposes of RFA.[35] These small entities hold approximately $540 billion in assets, accounting for 14 percent of total assets held by FDIC-supervised institutions. In addition, the rule affects all bank service providers that provide services subject to the BSCA.[36] The FDIC is unable to estimate the number of affected bank service providers that are small. For purposes of this certification, the FDIC assumes, as an upper limit, that all affected bank service providers are small.

[33] The SBA defines a small banking organization as having $600 million or less in assets, where an organization's assets are determined by averaging the assets reported on its four quarterly financial statements for the preceding year. *See* 13 CFR 121.201 (as amended by 84 FR 34261, effective August 19, 2019). In its determination, the SBA counts the receipts, employees, or other measure of size of the concern whose size is at issue and all of its domestic and foreign affiliates. *See* 13 CFR 121.103. Following these regulations, the FDIC uses a banking organization's affiliated and acquired assets, averaged over the preceding four quarters, to determine whether the banking organization is "small" for the purposes of RFA.

[34] FDIC Call Reports, June 30, 2020

[35] *Id.*

[36] Discussed in detail in the Impact Analysis section.

The proposed rule would require a banking organization to notify its primary federal regulator as soon as possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred. As described in the Impact Analysis section above, this requirement is estimated to affect a relatively small number of FDIC-supervised institutions and impose a compliance cost of up to three hours per incident. The agencies believe that the regulatory burden of such a requirement would be *de minimis* in nature, since the internal communications that led to the determination of the notification incident would have occurred regardless of the proposed rule.[37]

In addition, the proposed rule would require a bank service provider, as defined herein and in accordance with the BSCA, to notify at least two individuals at affected banking organization customers immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair the provision of services subject to the BSCA for four or more hours. As described in the Impact Analysis section above, the agencies believe that any additional compliance costs would be *de minimis* for each affected bank service provider.

Given that the costs of the proposed rule would be nominal or *de minimis*, the FDIC certifies that the proposed rule would not have a significant economic impact on a substantial number of small entities. The FDIC invites comments on all aspects of the supporting information provided in this RFA section. In particular, would this proposed rule have any significant effects on small entities that the FDIC has not identified?

Plain Language

[37] Even at an elevated labor compensation rate of $200 per hour, the proposed rule would impose a cost burden of less than $600 per incident.

Section 722 of the GLBA[38] requires the agencies to use plain language in all proposed and final rules published after January 1, 2000. The agencies have sought to present the proposed rule in a simple and straightforward manner and invite comment on the use of plain language. For example:

1. How could the agencies organize the material to better suit your needs? How could they present the proposed rule more clearly?
2. How could the requirements in the proposed rule be more clearly stated?
3. Do the regulations contain technical language or jargon that is not clear? If so, which language requires clarification?
4. Would a different format (grouping and order of sections, use of headings, paragraphing) make the regulation easier to understand? If so, what changes would achieve that?
5. Would more, but shorter, sections be better? If so, which sections should be changed?
6. What other changes can the agencies incorporate to make the regulation easier to understand?

OCC Unfunded Mandates Reform Act of 1995 Determination

The OCC analyzed the proposed rule under the factors set forth in the Unfunded Mandates Reform Act of 1995 (UMRA) (2 U.S.C. 1532). Under this analysis, the OCC considered whether the proposed rule includes a federal mandate that may result in the expenditure by State, local, and Tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year, adjusted for inflation (currently $157

[38] Codified at 12 U.S.C. 4809.

million). As noted in the OCC's Regulatory Flexibility analysis, the OCC expects that the costs associated with the proposal, if any, would be *de minimis* and, thus, has determined that this proposed rule would not result in expenditures by State, local, and Tribal governments, or the private sector, of $157 million or more in any one year. Accordingly, the OCC has not prepared a written statement to accompany this proposal.

Riegle Community Development and Regulatory Improvement Act of 1994

The Riegle Community Development and Regulatory Improvement Act of 1994 (RCDRIA)[39] requires that each federal banking agency, in determining the effective date and administrative compliance requirements for new regulations that impose additional reporting, disclosure, or other requirements on insured depository institutions, consider, consistent with principles of safety and soundness and the public interest, any administrative burdens that such regulations would place on depository institutions, including small depository institutions, and customers of depository institutions, as well as the benefits of such regulations. In addition, new regulations and amendments to regulations that impose additional reporting, disclosure, or other new requirements on insured depository institutions generally must take effect on the first day of a calendar quarter that begins on or after the date on which the regulations are published in final form.[40] The agencies invite comments that further will inform their consideration of the RCDRIA.

[39] Pub. L. 103-325, 108 Stat. 2160.
[40] 12 U.S.C. 4802(b)(1).

List of Subjects

12 CFR Part 53

Administrative practice and procedure, National Banks, Federal Savings Associations, Reporting and recordkeeping requirements, Safety and soundness.

12 CFR Part 225

Administrative practice and procedure, Bank holding companies, banking, Edge and agreement corporations, Foreign banking organizations, Savings and loan holding companies, Reporting and recordkeeping requirements, State member banks, Safety and soundness.

12 CFR Part 304

Administrative practice and procedure, Bank deposit insurance, Banks, banking, Reporting and recordkeeping requirements, Safety and soundness.

Authority and Issuance

For the reasons stated in the Common Preamble and under the authority of 12 U.S.C. 1, 93a, 161, 481, 1463, 1464, 1861–1867, and 3102, the Office of the Comptroller of the Currency proposes to amend chapter I of Title 12, Code of Federal Regulations, as follows:

1. Part 53 is added to read as follows:

PART 53—COMPUTER-SECURITY INCIDENT NOTIFICATION

Sec.

Authority: 12 U.S.C. 1, 93a, 161, 481, 1463, 1464, 1861–1867, and 3102.

§ 53.1 Authority, purpose, and scope.

(a) *Authority.* This part is issued under the authority of 12 U.S.C. 1, 93a, 161, 481, 1463, 1464, 1861–1867, and 3102.

(b) *Purpose.* This part promotes the timely notification of significant computer-security incidents that affect OCC-supervised institutions and their service providers.

(c) *Scope.* This part applies to all national banks, Federal savings associations, and Federal branches and agencies of foreign banks. This part also applies to bank service providers, as defined in § 53.2(b)(2) of this part.

§ 53.2 Definitions.

(a) Except as modified in this part, or unless the context otherwise requires, the terms used in this part have the same meanings as set forth in 12 U.S.C. 1813.

(b) For purposes of this part, the following definitions apply—

(1) *Banking organization* means a national bank, Federal savings association, or Federal branch or agency of a foreign bank.

(2) *Bank service provider* means a bank service company or other person

providing services to a banking organization that is subject to the Bank Service Company Act (12 U.S.C. 1861–1867).

(3) *Business line* means products or services offered by a banking organization to serve its customers or support other business needs.

(4) *Computer-security incident* is an occurrence that—

(i) Results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or

(ii) Constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(5) *Notification incident* is a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair—

(i) 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;

(ii) 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

(iii) 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.

(6) *Person* has the same meaning as set forth at 12 U.S.C. 1817(j)(8)(A).

§ 53.3 Notification.

A banking organization must notify the OCC of a notification incident through any form of written or oral communication, including through any technological means, to a designated point of contact identified by the OCC. The OCC must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred.

§ 53.4 Bank service provider notification.

A bank service provider is required to notify at least two individuals at each affected banking organization customer immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the Bank Service Company Act (12 U.S.C. 1861–1867) for four or more hours.

Authority and Issuance

For the reasons stated in the Common Preamble and under the authority of 12 U.S.C. 321–338a, 1467a(g), 1818(b), 1844(b), 1861–1867, 3101 *et seq.*, and 5365 the Board proposes to amend chapter II of Title 12, Code of Federal Regulations, as follows:

1. Subpart N is added to read as follows:

Subpart N—COMPUTER-SECURITY INCIDENT NOTIFICATION

Sec.

§ 225.300 Authority, purpose, and scope.

(a) *Authority.* This subpart is issued under the authority of 12 U.S.C. 1, 321–338a, 1467a(g), 1818(b), 1844(b), 1861–1867, 3101 *et seq.*, and 5365.

(b) *Purpose.* This subpart promotes the timely notification of significant computer-security incidents that affect Board-supervised entities and their service providers.

(c) *Scope.* This subpart applies to all U.S. bank holding companies and savings and loan holding companies; state member banks; the U.S. operations of foreign banking organizations; and, Edge and agreement corporations. This subpart also applies to bank service providers, as defined in § 225.301(a)(2) of this subpart.

§ 225.301 Definitions.

(a) For purposes of this subpart, the following definitions apply—

Banking organization means a U.S. bank holding company; U.S. savings and loan holding company; state member bank; the U.S. operations of foreign banking organizations; and an Edge and agreement corporation.

Bank service provider means a bank service company or other person providing services to a banking organization that is subject to the Bank

Service Company Act (12 U.S.C. 1861–1867).

Business line means products or services offered by a banking organization to serve its customers or support other business needs.

Computer-security incident is an occurrence that (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Notification incident is a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair—

(i) 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;

(ii) 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

(iii) 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.

(b) [Reserved]

§ 225.302 Notification.

A banking organization must notify the Board of a notification incident through any form of written or oral communication, including through any technological means (e.g., email, telephone, text, etc.), to a designated point of contact identified by the Board (e.g., an examiner-in-charge, local supervisory office, or a cyber-incident operations center). The Board must receive this notification from a banking organization as soon as possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred.

§ 225.303 Bank service provider notification.

A bank service provider is required to notify at least two individuals at each affected banking organization customer immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided, subject to the Bank Service Company Act (12 U.S.C. 1861–1867), for four or more hours.

For the reasons stated in the Common Preamble, the Board of Directors of the Federal Deposit Insurance Corporation proposes to revise 12 CFR part 304 to add a subpart C, as follows.

Authority and Issuance

For the reasons stated in the Common Preamble, and under the authority of 12 U.S.C. 1463, 1811, 1813, 1817, 1819, and 1861–1867, the FDIC proposes to amend 12 CFR part 304 as

follows:

PART 304—FORMS, INSTRUCTIONS, AND REPORTS

1. Revise the authority citation for part 304 to read as follows:

Authority: 5 U.S.C. 552; 12 U.S.C. 1463, 1464, 1813, 1817, 1819, 1831, and 1861–1867.

2. Revise section 304.1 to read as follows:

§ 304.1 Purpose.

This subpart informs the public where it may obtain forms and instructions for reports, applications, and other submittals used by the FDIC, and describes certain forms that are not described elsewhere in FDIC regulations.

3. Reserve sections 304.15 through 304.20.

4. Add a new subpart C to read as follows:

Subpart C - COMPUTER-SECURITY INCIDENT NOTIFICATION

Sec.

§ 304.21 Authority, purpose, and scope.

(a) *Authority*. This subpart is issued under the authority of 12 U.S.C. 1463, 1811, 1813, 1817, 1819, and 1861–1867.

(b) *Purpose.* This subpart promotes the timely notification of significant computer-security incidents that affect FDIC-supervised institutions and their service providers.

(c) *Scope.* This subpart applies to all insured state nonmember banks, insured state licensed branches of foreign banks, and State savings associations. This subpart also applies to bank service providers, as defined in § 304.22(b)(2) of this subpart.

§ 304.22 Definitions.

(a) Except as modified in this subpart, or unless the context otherwise requires, the terms used in this subpart have the same meanings as set forth in 12 U.S.C. 1813.

(b) For purposes of this subpart, the following definitions apply.

(1) *Banking organization* means an FDIC-supervised insured depository institution, including all insured state nonmember banks, insured state-licensed branches of foreign banks, and State savings associations.

(2) *Bank service provider* means a bank service company or other person providing services to a banking organization that is subject to the Bank Service Company Act (12 U.S.C. 1861–1867).

(3) *Business line* means products or services offered by a banking organization to serve its customers or support other business needs.

(4) *Computer-security incident* is an occurrence that (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or

transmits; or (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

(5) *Notification incident* is a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair—

(i) 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;

(ii) 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

(iii) 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.

(6) *Person* has the same meaning as set forth at 12 U.S.C. 1817(j)(8)(A).

§ 304.23 Notification.

A banking organization must notify the FDIC of a notification incident through any form of written or oral communication, including through any technological means, to a designated point of contact identified by the FDIC. The FDIC must receive this notification from the banking organization as soon as possible and no later than 36 hours

after the banking organization believes in good faith that a notification incident has occurred.

§ 304.24 Bank service provider notification.

A bank service provider is required to notify at least two individuals at each affected banking organization customer immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the Bank Service Company Act (12 U.S.C. 1861–1867) for four or more hours.

5. Reserve sections 304.25 through 304.30.

Brian P. Brooks
Acting Comptroller of the Currency

[FRB signature block]

Federal Deposit Insurance Corporation.
By order of the Board of Directors.
Dated at Washington, DC, on December [XX], 2020.
James P. Sheesley,
Assistant Executive Secretary

[BILLING CODES: 4810-33-P; 6210-01-P; 6714-01-P]