COMPUTER-SECURITY INCIDENT FINAL RULE DRAFT

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- 1736]
RIN 7100-AG06

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 (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC).

ACTION: Final rule.

SUMMARY: The OCC, Board, and FDIC are issuing a final rule that requires a banking organization 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 later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

DATES: Effective date: April 1, 2022; Compliance date: May 1, 2022.

FOR FURTHER INFORMATION CONTACT:

OCC:

Patrick Kelly, Director, Critical Infrastructure Policy, (202) 649–5519, Carl Kaminski, Assistant Director, (202) 649–5490, or Priscilla Benner, Senior Attorney, Chief Counsel's Office, (202) 649–5490, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219.

Board:

Thomas Sullivan, Senior Associate Director, (202) 475-7656, 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, Christopher Danello, Senior Attorney, (202) 736-1960, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551, or at https://www.federalreserve.gov/apps/ContactUs/feedback.aspx, and click on *Staff Group, Regulations*.

FDIC:

Rob Drozdowski, Special Assistant to the Deputy Director (202) 898–3971, rdrozdowski@fdic.gov, Division of Risk Management Supervision; or John Dorsey, Counsel (202) 898–3807, jdorsey@fdic.gov, Graham Rehrig, Senior Attorney, (202) 898-3829, grehrig@fdic.gov, Legal Division.

SUPPLEMENTAL INFORMATION:

Table of Contents

I. Introduction

The OCC, Board, and FDIC (together, the agencies) are issuing a final rule to require that a banking organization[1] promptly notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as those terms are defined in the final

[1] For the OCC, "banking organizations" includes national banks, federal savings associations, and federal branches and agencies of foreign banks. For the Board, "banking organizations" includes 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. For the FDIC, "banking organizations" includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations. Each agency's definition excludes financial market utilities designated under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (designated FMUs).

rule. As described in more detail below, these incidents may have many causes. Examples include a large-scale distributed denial of service attack that disrupts customer account access for an extended period of time and a computer hacking incident that disables banking operations for an extended period of time.

Under the final rule, a banking organization's primary federal regulator must receive this notification as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. This requirement will help promote early awareness of emerging threats to banking organizations and the broader financial system. This early awareness will help the agencies react to these threats before they become systemic. The final rule separately requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours. This separate requirement will ensure that a banking organization receives prompt notification of a computer-security incident that materially disrupts or degrades, or is reasonably likely to materially disrupt or degrade, covered services provided by a bank service provider. This notification will allow the banking organization to assess whether the incident has or is reasonably likely to have a material impact on the banking organization and thus trigger the banking organization's own notification requirement.

II. Background

Computer-security incidents can result from destructive malware or malicious software (cyberattacks), as well as non-malicious failure of hardware and software, personnel errors, and other causes. Cyberattacks targeting the financial services industry have increased in frequency

and severity in recent years.[2] These cyberattacks can adversely affect banking organizations' networks, data, and systems, and ultimately their ability to resume normal operations.

Given the frequency and severity of cyberattacks on the financial services industry, the agencies believe that it is important that a banking organization's primary federal regulator be notified as soon as possible of a significant computer-security incident[3] that disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the banking organization's operations, result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector.[4] The final rule refers to these significant computer-security incidents as "notification incidents."[5] Timely notification is important as it would allow the agencies to (1) have early awareness of emerging threats to banking organizations and the broader financial system, (2) better assess the threat a notification incident poses to a banking organization and take appropriate actions to address the threat, (3) facilitate and approve requests from banking organizations for assistance through U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection (OCCIP),[6] (4) provide information and guidance to banking

---

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

[3] As defined by the final rule, a *computer-security incident* is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits. To promote uniformity of terms, the agencies have sought to align this term generally with an existing definition from the National Institute of Standards and Technology (NIST). *See* NIST, Computer Security Resource Center, *Glossary* (last accessed Sept. 20, 2021), *available at https://csrc.nist.gov/glossary/term/Dictionary*.

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

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

[6] 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

organizations, and (5) conduct horizontal analyses to provide targeted guidance and adjust supervisory programs.

Notification under the Bank Secrecy Act[7] and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[8] provide the agencies with awareness of certain computer-security incidents.[9] Nonetheless, these standards do not include all computer-security incidents of which the agencies, as supervisors, need to be alerted and would not always result in timely notification to the agencies.

To ensure that the agencies receive timely alerts of all relevant material and adverse incidents, the agencies issued a notice of proposed rulemaking (NPR or proposal) to establish computer-security incident notification requirements for banking organizations and their bank service providers.[10]

The proposal would have required banking organizations to notify their primary federal regulator within 36 hours of when they believed in good faith that a "computer-security incident" that rises to the level of a "notification incident" had occurred. As proposed, a "notification incident" was a computer-security incident that could materially disrupt, degrade, or impair the viability of the banking organization's operations, result in customers being unable to access

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 Oct. 15, 2021).

[7] *See* 31 U.S.C. 5311 *et seq.*; 31 CFR subtitle B, chapter X.

[8] *See* 15 U.S.C. 6801*;* 12 CFR pt. 30, app'x B, supp. A *(OCC);* 12 CFR part 208, app'x D-2, supp. A, 12 CFR 211.5(l), 12 CFR part 225, app'x. F, supp. A (Board)*;* 12 CFR part 364, app'x B, supp. A (FDIC).

[9] 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. This rule does not change that expectation.

[10] 86 FR 2299 (Jan. 12, 2021).

their deposit and other accounts, or impact the stability of the financial sector.[11] When drafting these proposed definitions, the agencies sought to align the terminology as much as possible with language used in the National Institute of Standards and Technology's (NIST) Computer Security Resource Center glossary.[12] This approach was intended to promote consistency with known cybersecurity terms and definitions and thereby reduce burden.

The proposal separately would have required a bank service provider that provided services subject to the Bank Service Company Act (BSCA)[13] 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 BSCA for four or more hours. This standard reflected the agencies' conclusion that the impact of computer-security incidents at bank service providers can flow through to their banking organization customers. The agencies also recognized, however, that a bank service provider may not be able to readily assess whether an incident rises to the level of a notification incident for a particular banking organization customer.

The notification requirement for bank service providers is important because banking organizations have become increasingly reliant on third parties to provide essential services. Such third parties may also experience computer-security incidents that could disrupt or degrade the provision of services to their banking organization customers or have other significant impacts on a banking organization. Therefore, a banking organization needs to receive prompt notification of computer-security incidents that materially disrupt or degrade, or are reasonably

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

[12] NIST is an agency of the U.S. Department of Commerce that works to develop and apply technology, measurements, and standards.

[13] 12 U.S.C. 1861–67.

likely to materially disrupt or degrade, these services because prompt notification will allow the banking organization to assess whether the incident has or is reasonably likely to have a material impact and trigger its own notification requirement.

A. Overview of Comments

The agencies collectively received 35 comments from banking and financial sector entities, third-party service providers, industry groups, and other individuals.[14] This section provides an overview of the general themes raised by commenters. The comments received on the proposal are further discussed below in the sections describing the final rule, including any changes that the agencies have made to the proposal in response to comments.

General Reaction and Need for a Rule

A majority of commenters supported the proposal, agreeing that providing prompt notice of significant incidents is an important aspect of safety and soundness, and they supported transparent and consistent notification from bank service providers to their banking organization customers. A number of these commenters offered suggestions to clarify certain aspects of the requirements or lessen the perceived burden. Commenters also generally supported the agencies' efforts to harmonize with existing definitions and notification standards. Four commenters opposed the proposal, contending that compliance would be burdensome or duplicative of existing requirements, and may impede banking organizations' and bank service providers' abilities to respond effectively to incidents.

"Computer-Security Incidents" That Can Trigger Potential Reporting

[14] Comments can be accessed at: *https://www.regulations.gov/document/OCC-2020-0038-0001* (OCC); *https://www.federalreserve.gov/apps/foia/ViewComments.aspx?doc_id=R-1736&doc_ver=1* (Board); and *https://www.fdic.gov/resources/regulations/federal-register-publications/2021/2021-computer-security-incident-notification-3064-af59.html* (FDIC).

As described above, the proposal would have required reporting of certain "computer-security incidents," defined to be consistent with the NIST definition. While several commenters supported aligning the definition with NIST's definition, most commenters asserted that the proposed definition was overly broad, could be tailored, and suggested different revisions to the proposed definition of computer-security incident. Specifically, a number of these commenters asserted that the definition should be based on actual, rather than "potential," harm and exclude violations of a banking organization's or a bank service provider's policies and procedures.

"Notification Incidents" Required To Be Reported

As described above, notification incidents are computer-security incidents that require notification to the agencies. Most commenters argued that the proposed definition of "notification incident" was overly broad and should be narrowed and only require reporting of incidents involving actual harm.[15] Commenters asserted that any definition should incorporate time, risk, and scale elements, which commenters viewed as critical. In addition, commenters urged the agencies to replace the "good faith" standard with a banking organization's or a bank service provider's "determination" or a reasonable basis to conclude that an incident had occurred, to provide a more objective and concrete standard.[16]

Timeframes for Notification

The agencies received comments on the timeframes described in the proposal for banking organizations to provide notification to their regulator and for bank service providers to provide notification to their banking organization customers. These comments focused both on the

[15] A commenter suggested that if a banking organization had mitigation strategies in place to offset the impact to a banking organization or its customers, the incident should not be considered a significant or critical incident and therefore should not be considered a notification incident. The commenter also stated that the agencies should indicate that an outage that lasts less than 48-hours in duration does not represent a "notification incident."

[16] Commenters contended that the "good faith" standard may be unclear, and the agencies should provide guidance on how to make the good faith determination. However, some commenters preferred the good faith standard over a "reasonably likely" standard.

amount of time provided to make the notification and the trigger that caused the time period to begin being measured. Commenters made a wide variety of suggestions, including recommendations to lengthen and shorten the periods and to provide further clarity regarding when they commenced.

Means of Bank Service Provider Notification

Commenters raised questions regarding the requirement in the proposal that a bank service provider must notify two individuals at each affected banking organization. Notably, some commenters raised concerns that such a requirement would override contractual notification provisions with which both the bank service providers and banking organizations are comfortable.

Applicability to Financial Market Utilities

Commenters suggested that the proposal would cause unintended regulatory overlap for those financial market utilities that are designated as systemically important under Title VIII of the Dodd-Frank Act (designated FMUs) and regulated by the Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC). In addition, designated FMUs regulated by the Board are subject to Regulation HH, which includes risk-management standards.

III. Discussion of Final Rule

A. Overview of the Final Rule

In response to comments received on the NPR, the final rule reflects changes to key definitions and notification provisions applicable to both banking organizations and bank service providers. These changes include (1) narrowing the definition of computer-security incident by focusing on actual, rather than potential, harm and by removing the second prong of the

proposed definition relating to violations of internal policies or procedures; (2) substituting the phrase "reasonably likely to" in place of "could" in the definition of notification incident; and (3) replacing the "good faith belief" notification standard with a determination standard. Changes to the bank service provider notification provision include (1) adding a definition of "covered services" and (2) requiring that notice be provided to a bank-designated point of contact, rather than to at least two individuals at each banking organization customer. The final rule also excludes designated FMUs from the definitions of "banking organization" and "bank service provider."[17] Such changes are intended to address comments and reduce over- and unnecessary notification by both banking organizations and bank service providers.

The final rule establishes two primary requirements, which promote the safety and soundness of banking organizations and are consistent with the agencies' authorities to supervise these entities, and with their authorities pursuant to the BSCA.[18] First, the final rule requires a banking organization to notify its primary federal regulator of a notification incident. In particular, a banking organization must 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 later than 36 hours after the banking organization determines that a notification incident has occurred.[19] Second, the final rule requires a bank service provider[20] to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible

[17] The rule defines "designated financial market utility" as having the same meaning as set forth at 12 U.S.C. 5462(4).
[18] *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, and 3101 *et seq.* (Board); 12 U.S.C. 1463, 1811, 1813, 1817, 1819, and 1861–1867 (FDIC).
[19] As also noted below, however, the agencies would encourage those banking organizations providing sector-critical services that currently notify their primary federal regulator of these types of incidents on a same-day basis to continue to do so.
[20] As a general matter, "bank service provider" refers to a company or person that performs services for a banking organization that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867). However, for the purpose of this final rule, the term "bank service provider" does not include any person or company that is a designated FMU, as that term is defined at 12 U.S.C. 5462(4).

when the bank service provider determines it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization customer for four or more hours. Each of these requirements is discussed in more detail below.

B. Definitions

i. Definition of Banking Organization

The final rule applies to the following banking organizations:

- For the **OCC**, "banking organizations" includes national banks, federal savings associations, and federal branches and agencies of foreign banks.
- For the **Board**, "banking organizations" includes 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.
- For the **FDIC**, "banking organizations" includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations.
- For all three agencies, "banking organizations" does not include designated FMUs, for the reasons discussed below.[21]

With respect to the proposed definition of "banking organization," commenters suggested that this term should include additional entities, such as financial technology firms and non-bank OCC-chartered financial services entities, to the extent the agencies have jurisdiction over those firms. Further, commenters contended that the agencies should consider other regulatory frameworks to which banking organizations and bank service providers may already be subject

[21] Under the final rule, "designated financial market utility" has the same meaning as set forth at 12 U.S.C. 5462(4).

and exclude entities subject to other, similar, regulatory reporting requirements.[22] The agencies have defined the term banking organization in a manner that is consistent with the agencies' supervisory authorities.

The NPR solicited comment on the scope of entities that should be included as "banking organizations" for purposes of the rule, and specifically noted that the proposed rule's definition of "banking organizations" and "bank service providers" would include FMUs that are chartered as a State member bank or Edge corporation, or perform services subject to regulation and examination under the Bank Service Company Act.[23, 24] In that regard, the agencies asked whether there were unique factors that the agencies should consider in determining how notification requirements should apply to these FMUs. In addition, the agencies asked whether notification requirements would be best conveyed through the proposed rule or through amendments to the Board's Regulation HH for designated FMUs for which the Board is the Supervisory Agency under Title VIII of the Dodd-Frank Act.

In response to these requests for comment, two commenters opposed the application of the proposed rule to SEC-supervised FMUs that are designated as systemically important under Title VIII of the Dodd-Frank Act, arguing that the proposed rule would subject these designated FMUs to unintended regulatory overlap and duplicative compliance burdens. One of these commenters argued that SEC-supervised designated FMUs should be deemed to comply with the rule to the extent they comply with incident notification requirements under existing SEC

[22] For example, FMUs for which the SEC is the Primary Agency under Title VIII of the Dodd-Frank Act are subject to the SEC's Regulation SCI (Systems Compliance and Integrity) for certain financial intermediaries.
[23] An FMU is "any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person." 12 U.S.C. 5462(6).
[24] Title VIII of the Dodd-Frank Act authorizes the Financial Stability Oversight Council to designate certain FMUs as systemically important. Depending on the functions that it serves in the financial markets, a designated FMU is subject to risk-management regulations promulgated by the Board (i.e., Regulation HH), the SEC, or the CFTC.

regulations. Another commenter argued that applying the proposed rule to Board-supervised designated FMUs would be preferable to amending Regulation HH to include a designated FMU-specific incident notification requirement, but this commenter did not provide a detailed rationale for that position. Finally, several commenters suggested that the final rule should exempt all FMUs that qualify as a banking organization or a bank service provider, including FMUs that have not been designated as systemically important under Title VIII of the Dodd-Frank Act, from these incident notification requirements, arguing that the existing practice among FMUs is to alert supervisors directly in the case of computer-security incidents.

As noted above, the final rule excludes designated FMUs from the definitions of "banking organization" and "bank service provider."[25] In the case of SEC- and CFTC-supervised designated FMUs, the agencies determined that excluding these designated FMUs from the final rule is appropriate because these designated FMUs are already subject to incident notification requirements in other federal regulations.[26]

Board-supervised designated FMUs are subject to the Board's Regulation HH, which includes a set of risk-management standards for addressing areas such as legal risk, governance, credit and liquidity risks, and operational risk. Regulation HH requires generally that a Board-supervised designated FMU effectively identify and manage operational risks.[27] Although Regulation HH does not currently impose specific incident-notification requirements, the Board

[25] The rule defines "designated financial market utility" as having the same meaning as set forth at 12 U.S.C. 5462(4).

[26] Specifically, SEC-supervised designated FMUs are subject to the SEC's Regulation SCI, which generally requires covered entities to notify the SEC and their members or participants in the event of an SCI event. *See* 17 CFR 242.1000 (defining "SCI Event") and 242.1002 (imposing notification requirements related to SCI Events). Similarly, a CFTC-supervised designated FMU must notify the CFTC in the event of an "exceptional event" or the activation of the designated FMU's business continuity and disaster recovery plan. *See* 17 CFR 39.18(g). An "exceptional event" includes "[a]ny hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity." *Id.*

[27] 12 CFR 234.3(a)(17).

believes that it is important for designated FMUs to inform Federal Reserve supervisors of operational disruptions on a timely basis and has generally observed such practice by the designated FMUs. The Board will continue to review Regulation HH in light of designated FMUs' existing practices and may propose amendments to Regulation HH in the future to formalize its incident-notification expectations and promote consistency between requirements applicable to Board-, SEC-, and CFTC-supervised designated FMUs.

Although some commenters suggested that the final rule should exempt all FMUs that qualify as a banking organization or a bank service provider, the agencies have adopted a narrower exclusion for designated FMUs.[28] FMUs that are not designated and that otherwise meet the definition of banking organization or bank service provider are within the rule's scope. The agencies determined that excluding all FMUs from the rule would be overly broad and would result in the inconsistent regulatory treatment of FMUs that are not designated relative to other bank service providers. In addition, a broad FMU exclusion could create uncertainty because there is no defined list of FMUs, other than designated FMUs.

One commenter suggested that the Board should hold Federal Reserve Bank Services to an equivalent standard as a matter of fairness and competitive equality. Given that designated FMUs are scoped out of this rule, the Federal Reserve Banks' retail payment and settlement services are the only relevant Federal Reserve Bank Services that compete with those private-sector FMUs that are subject to the final rule.[29] These retail services currently include check

[28] This narrow exclusion would not apply to a Board-supervised designated FMU with respect to its operation of non-systemically important services that are not subject to Regulation HH.

[29] The Federal Reserve Banks also operate the Fedwire Funds Service and Fedwire Securities Service, which play a critical role in the financial system. The Board generally requires these services to meet or exceed the risk-management standards applicable to designated FMUs under Regulation HH. *See Federal Reserve Policy on Payment System Risk* (as amended effective Mar. 19, 2021), *https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf*. See also Press Release, *Federal Reserve Board Reaffirms Long-Standing Policy of Applying Relevant International Risk-Management Standards to Fedwire*

collection services for depository institutions and an automated clearinghouse service that enables depository institutions to send batches of debit and credit transfers. For these services, the Federal Reserve Banks follow protocols to ensure timely communication of incidents to both depository institution customers and the Board. The Board believes these protocols are comparable to those required by this final rule. With respect to future Federal Reserve Bank Services that compete with private-sector FMUs subject to the final rule (such as the FedNow Service), the Board intends to similarly hold the Federal Reserve Banks to protocols comparable to those required by this final rule.

ii. Definition of Bank Service Provider

The agencies sought feedback on the scope of third-party services covered under the proposed rule and whether the proposed rule's definition of "bank service provider" appropriately captured the services about which banking organizations should be informed in the event of disruptions. The agencies further sought comment on whether all services covered under the BSCA should be included for purposes of the notification requirement or whether only a subset of the BSCA services should be included. The agencies also sought comment on whether only examined bank service providers should be subject to the notification requirement.

With respect to the definition of "bank service provider," commenters expressed varied opinions on the scope of entities included in the definition of "bank service provider." Some commenters argued that the definition should be revised to clarify that only service providers providing services that are subject to the BSCA would be subject to the rule, and one commenter suggested that the agencies provide a non-exclusive list of categories of bank service providers subject to the regulation. Other commenters urged that bank service providers should include

---

Funds and Fedwire Securities Services (July 19, 2012), *https://www.federalreserve.gov/newsevents/pressreleases/bcreg20120719a.htm*.

entities with access to bank customer information or systems, whether or not formally within the scope of the BSCA, while one commenter recommended excluding banking organization subsidiaries and affiliates. Some suggested that the agencies narrow the scope to apply only to significant service providers, bank service providers that present a higher risk, or those that provide technology services. Other commenters suggested excluding bank service providers from the rule entirely, observing that incident notification is, and should be, addressed in contracts.

The agencies agree that bank service providers providing services that are subject to the BSCA should be subject to the rule. The agencies disagree with the rest of these suggestions to modify the scope of entities included in the definition of bank service provider. As previously explained, bank service providers play an increasingly important role in banking organization operations. Significant incidents affecting the services they provide have the potential to cause notification incidents for their banking organization customers. This risk is not limited to specific bank service providers, and therefore, the agencies decline to modify the scope of entities included in the definition in the manners suggested by the comments above.

Furthermore, while the agencies agree that incident notification is generally addressed by contract, we believe that this issue is important enough to warrant an independent regulatory requirement that ensures consistency and enforceability, without the necessity of revising contractual provisions.

In response to comments that the agencies should clarify the scope of bank service providers that would be subject to the rule, the agencies made changes to the final rule that do so. First, the agencies added a new definition in the final rule, "covered services," which definition is intended to clarify that services performed subject to the BSCA would be covered by the rule.

Second, as noted above, the agencies excluded designated FMUs from the definition of "bank service provider" and from the definition of "banking organization."[30] The final rule defines "bank service provider" as a bank service company or other person who performs covered services; provided, however, that no designated FMU shall be considered a bank service provider. "Covered services" are services performed by a "person"[31] that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867).

iii. Definition of Computer-Security Incident

In the NPR, the agencies generally incorporated the principal definition employed by NIST to define "computer-security incident" as follows:

"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.

Although commenters generally supported the agencies' use of a standard industry term rather than a new, and potentially inconsistent, term and definition, they suggested revisions to more closely tailor the definition to the purposes of the rule. For example, many commenters recommended that the definition focus on incidents that result in actual, rather than potential, harm to an information system. Commenters were concerned that the tracking and notification of incidents that could potentially harm a banking organization would create an undue regulatory

[30] The rule defines "designated financial market utility" as having the same meaning as set forth at 12 U.S.C. 5462(4).
[31] The final rule states that "person" has the same meaning as set forth at 12 U.S.C. 1817(j)(8)(A).

burden, possibly result in over-notification, and overlook the fact that many potential incidents can be effectively remediated. In addition, various commenters recommended deleting the second prong of the proposed definition, reasoning that violations of internal policies and procedures would be unlikely ever to result in incidents significant enough to warrant prompt notification; however, some commenters supported keeping actual violations of applicable security policies. Commenters also suggested introducing materiality thresholds or excluding non-security related outages or incidents. One commenter objected to narrowing the definition to "actual" harm and supported broadening the definition to include incidents causing "serious," but not necessarily "imminent," harm. Another commenter stated that the standard for determining whether an incident rises to the level to trigger mandated notices should be based on its impact to banking organizations or the financial system and be agnostic as to cause. One commenter stated that the definition should expressly exclude scheduled outages. The same commenter suggested that the term computer-security incident be changed to encompass two types of outages and align more with the NIST definition of cybersecurity incident to provide greater uniformity and clarity about what constitutes an incident and a reportable incident. Another commenter also suggested substituting the term cybersecurity incident from NIST in lieu of computer-security incident. A commenter also suggested narrowing the term "incident" to exclude non-malicious data communications incidents or those occurring outside of the regulated entity's own network.

While the agencies continue to recognize that there is value in adopting an existing, standard definition, the agencies agree that the NIST definition does not wholly align with the purposes of the rule. The agencies have therefore narrowed the final rule's definition of "computer-security incident," as suggested by the foregoing comments. Specifically, the final

rule defines "computer-security incident" as an occurrence that results in actual harm to an information system or the information contained within it.[32] Furthermore, the agencies have removed the second prong of the proposed computer-security incident definition relating to violations of internal policies or procedures. These changes narrow the focus of the final rule to those incidents most likely to materially and adversely affect banking organizations, while still retaining general consistency with the NIST definition.[33]

iv. Definition of Notification Incident

The NPR defined a "notification incident" as 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.

---

[32] One commenter requested clarification as to whether a "near-miss" incident would constitute a computer-security incident under the rule. A "near-miss" incident would constitute a computer-security incident only to the extent that such a "near-miss" results in actual harm to an information system or the information contained within it. Another commenter stated that the definition of "computer-security incident" should be limited to information systems that can cause a "notification incident." For clarification, the definition of "computer-security incident" includes all occurrences that result in actual harm to an information system or the information contained within it. However, only those computer-security incidents that fall within the definition of "notification incident" are required to be reported. Two commenters advocated for excluding computer-security incidents due to non-security and non-malicious causes. For clarity, the definition includes incidents from whatever cause.

[33] In response to comments, the agencies also considered whether to incorporate the NIST definition of "cybersecurity incident" instead and determined that this definition would inappropriately narrow the scope of incidents covered by the rule.

Commenters addressed several aspects of the proposed definition. First, multiple commenters observed that the term "could" in the phrase "could … disrupt, degrade, or impair" was imprecise and overbroad. Multiple commenters suggested substituting the phrase "could" with "reasonably likely to or will" materially disrupt certain business lines or operations or "has resulted in or will result in" material disruptions to certain business lines or operations in its place. Some commenters also suggested that "notification incident" should be narrowed even further to incidents that actually materially disrupt or degrade.[34]

The agencies also received a number of comments on the NPR's "believes in good faith" language. Various commenters expressed support for the phrase, with at least one noting that the more subjective "good faith" standard gave some flexibility to an organization that might honestly, albeit mistakenly, conclude that an occurrence did not rise to the level of a notification incident and thereby fail to provide notice.[35] Other commenters suggested that "believe in good faith" was too subjective and stated that the final rule should substitute a clearer term, such as "determined."[36] And one commenter suggested that the agencies change the "in good faith" belief notification standard to apply to critical, not significant, incidents.

In addition, commenters suggested that the final rule should specifically exclude from the notification requirement incidents where the impact is limited to certain types of computer systems (e.g., compromises to a bank's marketing or personnel systems) or otherwise provide

[34] A commenter suggested that if a banking organization had mitigation strategies in place to offset the impact to a bank or its customers, the incident should not be considered a significant or critical incident and therefore should not be considered a notification incident. The commenter also stated that the agencies should indicate that an outage that lasts less than 48-hours in duration does not represent a "notification incident."

[35] Two commenters supported maintaining the "good faith" standard, with one commenter noting that a reasonable belief standard could introduce too much uncertainty and invite questioning of decisions that are made quickly out of necessity and potentially without key facts known. One of those commenters stated that the final rule should reflect that information may not be available to make an assessment "immediately" after an occurrence.

[36] Commenters contended that the "good faith" standard may be unclear, and the agencies should provide guidance on how to make the good faith determination. An alternative would be for the rule text to state "an incident that a banking organization determines is reasonably likely to disrupt" instead of "believes in good faith could disrupt." However, some commenters preferred the good faith standard over a "reasonably likely" standard.

specific exclusions (e.g., any incident lasting less than 48 hours), because they would be very unlikely to cause the kinds of harm that the agencies would regard as warranting notification. Another commenter suggested that the agencies include a requirement that a notification incident involve an information system operated by, or on behalf of, a banking organization, because it would be unduly burdensome and potentially unrealistic for covered entities to be responsible for systems operated by third parties, whereas another commenter believed the term "notification incident" should be revised to include incidents occurring at third-party service provider information systems and the sub-contractors (fourth-party providers) of those third-party service providers that collect banking-related information. One commenter recommended that the agencies use the same definition of notification incident for bank service providers and banking organizations, whereas another commenter stated that only "notification incidents" should be reported under the rule to ensure that high volumes of less significant or easily remediated occurrences and incidents that do not result in actual harm are not reported. In addition, one commenter stated that banking organizations should not be required to publicly disclose core business lines and critical operations to avoid inviting attacks. Another commenter supported the definition and suggested that the definition of notification incident be expanded to include events that involve infiltration of third-party systems that collect banking related information, such as password managers or browsers. Another commenter requested that the agencies clarify that voluntary reporting of incidents falling outside of the scope of the definition is permitted, and that the rule also distinguish between mandatory reporting of notification incidents and nondisruptive events that could be reported through an alternative, voluntary mechanism and timeline.

Following analysis and careful consideration of the various comments, the agencies are

finalizing the definition largely as proposed, with modifications to address a number of commenters' concerns to clarify the rule and make it easier to administer.

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.[37] In particular, the second prong of the notification incident definition identifies incidents that impact core business lines, and the third prong identifies incidents that impact critical operations. Banking organizations subject to the Resolution Planning Rule may use the "core business lines" and "critical operations" identified in their resolution plans[38] to identify notification incidents under the second and third prongs of the final rule.

The final rule does not require 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, all banking organizations must have a sufficient understanding of their lines of business to be able to determine which business lines would, upon failure, result in a material loss of revenue, profit, or franchise value to the banking organization, so that they can meet their notification obligations.

Commenters also requested that the agencies clarify that the material loss of revenue,

---

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

[38] Elements of both the "core business lines" and "critical operations" definitions from the Resolution Planning Rule are incorporated in the "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.

profit, or franchise value addressed by the second prong of the definition should be evaluated on an enterprise-wide basis. The agencies agree; a banking organization should evaluate whether the loss is material to the organization as a whole.

The agencies have concluded that there is substantial benefit to receiving notification of both computer-security incidents that have materially disrupted or degraded, and incidents that are reasonably likely to materially disrupt or degrade, a banking organization. Accordingly, the agencies are not narrowing the definition of "notification incident" to only include computer-security incidents that have resulted in a material disruption or degradation in the final rule.

However, the agencies are narrowing the scope of covered computer-security incidents by substituting the phrase "reasonably likely to" in place of "could." The agencies agree that the term "could" encompasses more, and more speculative, incidents than the agencies intended in promulgating the rule. Accordingly, and in keeping with commenters' suggestions, the agencies have substituted the term "reasonably likely to" in place of "could." Under the "reasonably likely" standard, a banking organization will be required to notify its primary federal regulator when it has suffered a computer-security incident that has a reasonable likelihood of materially disrupting or degrading the banking organization or its operations, but at the same time would not be required to make such a notification for adverse outcomes that are merely possible, or within imagination. The "reasonably likely" standard for notification is clearer and more in line with the agencies' intentions for the rule. Finally, the agencies believe that banking organizations are well-positioned to assess the likelihood that a computer-security incident will result in the significant adverse effects described in the definition.

Some commenters also observed that the term "impair" was redundant of "disrupt" and "degrade;" that it was not a term defined by NIST; and that it should be removed. The agencies

agree the term would be redundant with "disrupt or degrade," and have removed the term "impair" from the definition.

After considering the comments carefully, the agencies are replacing the "good faith belief" standard with a banking organization's determination. The agencies agree with commenters who criticized the proposed "believes in good faith" standard as too subjective and imprecise. Accordingly, the agencies have removed the good faith language from the definition of "notification incident" and have substituted a determination standard in the final notification requirement.

Finally, the agencies decline to exclude particular incidents or incidents that impact certain types of computer systems from the notification requirements. The agencies believe that the focus on the material adverse effects of a computer-security incident is a simpler and clearer way to ensure that they receive notification of the most significant computer-security incidents.

v. Examples of Notification Incidents

The NPR included a non-exhaustive list of incidents that would be considered notification incidents under the proposed rule and the agencies invited comment on specific examples of computer-security incidents that should or should not constitute notification incidents. The agencies received a few general comments about the list of incidents.

One commenter suggested that the agencies include additional details in the illustrative examples that would identify the type of information systems that would not require incident notification and another suggested more broadly that the final rule include illustrative examples of both incidents that would and would not be subject to the final rule. The agencies believe that the criteria set forth in the notification incident definition make clear that the focus of the rule is on incidents that materially and adversely impact a banking organization rather than on specific

types of information systems. The agencies recognize that many banking organizations manage computer-security incidents every day that would not require notification under the final rule and have focused on illustrative examples of the type of incidents that would require notification.

One commenter suggested that the example discussing a ransom malware attack that encrypts a banking organization's core system is "duplicative of various federal and state breach notification laws." The agencies continue to conclude that any incident of ransom malware that disrupts a banking organization's ability to carry out banking operations meets the definition of a notification incident, and as such, have retained this example, notwithstanding any potential overlap between the final rule and other federal and state requirements for incident reporting.[39]

Another commenter suggested that some of the examples provided were "inconsistent with" the term computer-security incident, as incidents such as failed system upgrades or unrecoverable system failures are not technically computer-security incidents. The agencies disagree with this comment and believe that the commenter is reading the definition of computer-security incident too narrowly to focus on malicious incidents.

The agencies believe the examples in the proposed rule provide an appropriate perspective on the critical nature of the type of incidents that banking organizations should consider notification incidents. Having received only general comments and no specific new examples of notification incidents that should be included in the list, the agencies are retaining the illustrative examples provided in the NPR with some minor edits.[40]

---

[39] As previously explained, the agencies have considered whether existing reporting standards meet the purposes of this rule and concluded that they do not. For example, ransom malware incidents that do not involve unauthorized access to or use of sensitive customer information would not be subject to the GLBA notification standard.

[40] This is to clarify that example 6 addresses malware on a banking organization's system that poses *an imminent threat to the banking organization's core business lines or critical operations* or that requires the banking organization to disengage *any compromised products or information systems that support the banking organization's core business lines or critical operations from* Internet-based network connections.

The following is a non-exhaustive list of incidents that generally are considered "notification incidents" under the final 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;
3. A failed system upgrade or change that results in widespread user outages for customers and banking organization 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 on a banking organization's network that poses an imminent threat to the banking organization's core business lines or critical operations or that requires the banking organization to disengage any compromised products or information systems that support the banking organization's core business lines or critical operations from Internet-based network connections; and
7. A ransom malware attack that encrypts a core banking system or backup data.

While the agencies have included these illustrative examples to help clarify the scope of notification incidents, the final rule requires banking organizations to consider, on a case-by-case basis, whether any significant computer-security incidents they experience constitute notification incidents for purposes of notifying the appropriate agency. If a banking organization is in doubt

as to whether it is experiencing a notification incident for purposes of notifying its primary federal regulator, the agencies encourage it to contact its regulator. The agencies recognize that a banking organization may file a notification, from time to time, upon a mistaken determination that a notification incident has occurred, and the agencies generally do not expect to take supervisory action in such situations.

C. Banking Organization Notification to Agencies

i. Timing of Notification to Agencies

The proposed rule would have required banking organizations to provide the mandated notification to the agencies as soon as possible and no later than 36 hours. The agencies asked whether this timeframe should be modified, and if so, how.

One commenter suggested that the agencies eliminate the "as soon as possible" requirement and simply require notification within 36 hours, which would eliminate an apparent tension between the permission for an organization to take a reasonable amount of time to determine that it has experienced a notification incident and the requirement for immediate reporting. Some commenters supported the 36-hour timeframe as an appropriate balance between the potential burden on institutions and the agencies' need for prompt information.[41] However, other commenters expressed concerns, viewing the 36-hour timeframe as too short to allow a banking organization to fully understand a computer-security incident and to provide a complete assessment of the situation. Commenters noted that the 36-hour timeframe is only workable when it commences after a banking organization determines that a notification incident has occurred. In this regard, two commenters requested that the agencies expressly articulate in

[41] One commenter suggested that notification obligations should begin "36 hours after the banking organization confirms a notification incident has occurred, and has completed urgent measures to end the threat and protect its assets," to include time for a banking organization to take necessary measures.

the final rule the explanation included in the NPR that the 36-hour timeframe commences at the point when a banking organization has determined that a notification incident has occurred. Several commenters suggested that the agencies consider a 72-hour window to provide banking organizations with additional time to assess potential incidents and to align the proposed rule with other regulatory requirements such as the New York State Department of Financial Services' (NYDFS) cybersecurity event notification requirement,[42] or the European Union's General Data Protection Regulation (GDPR),[43] both of which require covered entities to report relevant cyber-related incidents within 72 hours.[44] A few commenters suggested that the notification timeframe should be increased to 48 hours, with one suggesting that any timeline align with business day processing, and another observing that community banks "need the additional 12 hours to evaluate the situation and implement an appropriate incident response plan." One commenter suggested that the notification timeframe be extended to a minimum of five business days for banks under $20 billion in assets in order to "provide banks adequate time to work with vendors and their core processors to provide accurate notifications." Another commenter observed that, "for a 36-hour notification timeframe to be potentially workable and achievable, it is imperative that the scope of the notification requirement be tailored."

The agencies continue to believe that 36 hours is the appropriate timeframe, given the

---

[42] Effective March 1, 2017, the NYDFS Superintendent promulgated 23 NYCRR Part 500, a regulation establishing cybersecurity requirements for financial services companies. Section 500.17 *Notices to superintendent* requires each "covered entity" to notify the NYDFS Superintendent "as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred." The NYDFS regulation is available at: *https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)*.

[43] In particular, Article 33, Section 1 of the GDPR provides that, in the case of a personal data breach, the data controller "shall without undue delay and, where feasible, not later than 72 hours after having become aware of it," notify the competent supervisory authority of the personal data breach. Moreover, Article 33, Section 2 requires data processors to "notify the [data] controller without undue delay after becoming aware of a personal data breach." The full version of Regulation (EU) 2016/679 (GDPR) is available at: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679*.

[44] *See id*.

simplicity of the notification requirement and the severity of incidents captured by the definition of "notification incident."[45] In developing the NPR and final rule, the agencies reviewed a number of existing security incident reporting requirements cited by the commenters and found that many of them involved detailed, prescriptive reporting requirements, often mandating that specific information be reported and including filing instructions. For example, the NYDFS rule requires that covered entities submit an annual statement certifying their compliance with the rule and keep all documents supporting their certification for five years, among other things. In contrast, the final rule sets forth no specific content or format for the simple notification it requires. The final rule is designed to ensure that the appropriate agency receives timely notice of significant emergent incidents, while providing flexibility to the banking organization to determine the content of the notification. Such a limited notification requirement will alert the agencies to such incidents without unduly burdening banking organizations with detailed reporting requirements, especially when certain information may not yet be known to the banking organizations.

In addition, changes to the definitions of "computer-security incident" and "notification incident" described above narrow the range, and reduce the speculative or uncertain nature of, incidents subject to the notification requirement.

The narrowed scope of notification incidents, however, makes it even more important for the agencies to receive notice as soon as possible. Additionally, 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

[45] As noted above, the agencies recognize that a banking organization may file a notification, from time to time, upon a mistaken determination that a notification incident has occurred, and the agencies generally do not expect to take supervisory action in such situations.

primary federal regulator. The agencies believe, however, that 36 hours is a reasonable amount of time after a banking organization has determined that a notification incident has occurred to notify its primary federal regulator, as it does not require an assessment or analysis.

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. For example, some notification incidents may occur outside of normal business hours. Only once the banking organization has made such a determination would the 36-hour timeframe begin.

Accordingly, the agencies have determined that the final rule will retain the requirement that banking organizations provide notice as soon as possible and no later than 36 hours. The agencies note, however, that even within the 36-hour notification window, banking organizations' notification practices should take into account their criticality to the sector in which they operate and provide services. An effective practice of banking organizations that provide sector-critical services is to provide same-day notification to their primary federal regulator of a notification incident. The agencies encourage this practice to continue among these banking organizations.

ii. Method of Notification to Agencies

The proposed rule would have required a banking organization to notify the appropriate agency 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 agency.

The agencies requested comments on how banking organizations should provide notifications to the agencies and sought comment on whether they should "adopt a process of

joint notification" where multiple banking organization affiliates have differing notification obligations. Further, the agencies requested feedback on how such a joint notification should be done and why.

A substantial number of commenters responded to various aspects of these questions. While specific suggestions varied, a consistent theme was a desire for efficient and flexible options for providing notice, with some commenters observing that a notification incident could also affect normal communication channels. Other commenters made recommendations to enhance notification efficiency, such as suggesting the use of automated electronic notifications. Two commenters suggested that, consistent with the agencies' statement in the NPR, the rule should explicitly state that no specific information is required and that the rule does not prescribe any particular reporting form.

The agencies have concluded that email and telephone are the best methods currently available for effective notification. Recognizing, however, that agency processes may evolve and technology will likely change (and improve) available communication options over time, the agencies have also built flexibility into the final rule by stating that the agencies may prescribe other similar methods pursuant to which notice may be provided. The agencies believe that this approach balances the need for banking organizations to have some flexibility, including if a communication channel is impacted by the incident, with the agencies' need to ensure that they actually receive the notifications.

The agencies also sought comments on whether centralized points of contact, regional offices, or banking organization-specific supervisory teams would be better suited to receive these notifications. The comments from banking organizations and bank service providers differed on this issue.

Some banking organizations suggested that the process should remain "flexible" and that the rule provide that the notification requirement could be "satisfied by any of several methods," including providing the notification to the banking organization's on-site or supervisory teams, appropriate regional offices, or an agency-designated point of contact. Other commenters, including bank service providers, suggested creating a joint notification process, or centralized portal or point of contact for all agencies to receive all such notifications directly. The agencies believe that the provision of notice can often be efficiently and effectively achieved by communicating with the appropriate agency supervisory office or other designated agency contacts, which may include designated supervisory staff, call centers, incident response teams, and other contacts to be designated by the respective agency.

The agencies also received several comments requesting further instruction and guidance on the method and manner of the required notifications. Several other commenters requested additional guidance on what a notice must contain and the scope of information that should be provided, and even requested certain specific exclusions.

The notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator about a notification incident. The agencies anticipate that banking organizations will share general information about what is known at the time of the incident. No specific information is required in the notification other than that a notification incident has occurred. The final rule does not prescribe any form or template. A simple notice can be provided to the appropriate agency supervisory office, or other designated point of contact, through email, telephone, or other similar method that the agency may prescribe. The notifications, and any information related to the incident, would be subject to the agencies'

confidentiality rules.[46]

Accordingly, the agencies revised the NPR language. The final rule provides that a banking organization would notify the appropriate agency-designated point of contact through email, telephone, or other similar methods that the agency may prescribe.

D. Bank Service Provider Notification to Banking Organization Customers

i. Scope of Bank Service Provider Notification

Commenters generally supported the idea of only notifying affected customers although some commenters suggested that all banking organization customers should be notified.[47] One commenter specifically suggested that bank service provider notifications should only go to banking organizations that are "directly impacted by the incident when a bank service provider has made a determination that the incident will or is reasonably likely to materially impact the services provided to the banking organization." The agencies agree with the "materiality" aspect of this comment and the focus on "reasonably likely" impacts. Accordingly, the agencies are revising the final rule to include the phrase "materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade." This change is also responsive to comments that requested the agencies further harmonize the bank service provider notification requirement with the banking organization notification requirement.

The final rule does not require a bank service provider to assess whether the incident rises to the level of a notification incident for a banking organization customer, which remains the responsibility of the banking organization. The agencies anticipate that bank service providers

[46] *See, e.g.*, 12 CFR pt. 4 (OCC); 12 CFR pt. 261 (Rules Regarding Availability of Information) (Board); 12 CFR 309.6 (Disclosure of exempt records) (FDIC).

[47] While most commenters believe that notifying all banking organizations subscribing to the disrupted service may lead to potentially harmful over-reporting, one commenter stated that notifying all banking organizations using the service may be appropriate since the service disruption may be broader than originally expected.

would make a best effort to share general information about what is known at the time. If, after receiving notice from a bank service provider, the banking organization determines that a notification incident has occurred, the banking organization is required to notify its primary federal regulator in accordance with this final rule. The agencies generally will not cite a banking organization because a bank service provider fails to comply with its notification requirement.

Another commenter described the potential for confusion that could ensue if a bank service provider were to notify all customers, when only some of them were affected by the computer-security incident. They advised that such an overly broad notification to all customers could "cause the banking organization customers and the bank service provider to respond to questions and concerns from banking organization customers [who were] not affected by the computer-security incident." The agencies agree with these commenters and are retaining in the final rule the requirement that notice be provided only to "each affected banking organization customer."

Another commenter noted that the final rule needs to account for the distinction between cloud-based services versus on-premises services and a shared-responsibility service delivery model. Under the final rule, the agencies would require bank service providers to continue to provide a banking organization customer with prompt notification of material incidents regardless of current contract language and irrespective of the chosen service delivery model. Even under a shared service model, a bank service provider will still need to provide notice to banking organization customers if the bank service provider has determined it has experienced a computer-security incident that has materially disrupted or degraded, or is likely to materially disrupt or degrade, covered services provided to such banking organization customer for four or

more hours. Given the purposes of the rule, the agencies believe this is a reasonable requirement and are adopting it in the final rule.

Whether the covered services are being provided through a software-as-a-service (SaaS) arrangement, or through some other service delivery method, a bank service provider must provide notification to banking organizations in accordance with the standard in the final rule. The banking organization must then independently determine if a notification incident has occurred.

Finally, in response to concerns expressed by commenters, the agencies are revising the final rule to specifically exclude scheduled maintenance, testing, or software updates previously communicated to a banking organization customer. This new exception should reduce over- and unnecessary notification. If, however, the scheduled maintenance, testing, or software update exceeds the parameters communicated to the banking organization customer and meets the notification standard set forth in the rule, this exception does not apply.

ii. Timing of Bank Service Provider Notification

Several commenters favored immediate notifications. Others were concerned that immediate notifications may result in over- and inaccurate notification. For example, some commenters objected to the requirement that a bank service provider must "immediately" notify affected banking organizations[48] and recommended that the notification occur "as soon as practicable," within the first four hours of the occurrence of a computer-security incident, or in a "timely" manner (or a similar standard) after a service disruption to prevent over-reporting and provide time for bank service providers to assess the severity of an incident.[49] One commenter

[48] Obstacles to immediate notification mentioned by commenters included that bank service providers need time to assess whether an incident is a computer-security incident.

[49] A commenter suggested that any timing for notification should allow an opportunity for reasonable investigation

noted that an immediate notification standard may be appropriate but only after the bank service provider determines that a notification incident has occurred, while other commenters stated that immediate notification was appropriate. Another commenter expressed concern that immediate notice may leave no time lapse "between when a computer-security incident occurred and when notification has to happen." While expressing similar sentiments, some commenters suggested substituting the term "timely," or "promptly" and "without undue delay," in place of the "immediate" requirement. Another commenter suggested that different reporting obligations should be permitted contingent upon the location of the incident (on-premise services vs. cloud services). The same commenter suggested modifying the "good faith" standard to instead require "prompt" notification where a bank service provider obtains actual knowledge of an incident that impacts services for more than four hours.

Other commenters drew distinctions between security incidents and service disruptions. One commenter observed that "[u]nlike a 'computer-security incident' which requires time to identify and evaluate, a disruption in service is instantaneously apparent and bank service providers can immediately notify banking organizations of the disruption in service." For similar reasons, another commenter suggested bifurcation of service provider notifications: "one immediate notice timeline if the incident affects the security of the banking organization's systems and a second, longer time period for disruption."

In response to these comments, the agencies are revising the rule to provide that a bank service provider must notify affected banking organization customers "as soon as possible" when it "determines" it has experienced an incident that meets the standard in the rule. Use of the term "determined" allows the bank service provider time to examine the nature of the incident and

---

to help ensure that material incidents are flagged to the regulators and are not obfuscated by an influx of false positives or non-material matter.

assess the materiality of the disruption or degradation of covered services. Additionally, the "four or more hours" threshold should reduce notifications concerning less material incidents. Once the bank service provider has made this determination, it must provide notice "as soon as possible."

Some commenters recommended revising the proposed rule to "allow for service providers to satisfy their notification requirement by providing notification to their banking customer consistent with any requirements and by any methods set forth in their contract with that customer, so long as the method reasonably ensures that the banking organization receives the notification." While the agencies believe it is reasonable to assume that providing notification to customers following a determination that a material incident has occurred should be consistent with many existing contractual provisions, the agencies conclude that an independent regulatory requirement is appropriate to ensure that banking organizations receive consistent and timely notification of the most significant computer-security incidents affecting covered services.

Other comments suggested that a 36- or 72-hour notification timeframe would be reasonable. For the reasons expressed above, the agencies disagree that bank service providers could (or should) wait this long to alert banking organization customers about a material disruption or degradation in covered services. Accordingly, the final rule requires bank service providers to provide notice as soon as possible when the bank service provider has determined it has experienced a notification incident.

iii. Bank Service Provider Notification to Customers

Some commenters stated that the requirement in the proposal to notify two individuals at each affected banking organization of an incident was appropriate. One commenter suggested

that a third notification be sent to a banking organization's general email or telephone number. Several commenters recommended the agencies allow the notification through general channels accessible by multiple employees at affected banking organizations, and one commenter suggested that "significant" bank service providers should directly notify the agencies. Other commenters asserted that requiring bank service providers to notify two contacts at each banking organization customer would be overly prescriptive and burdensome.[50] Instead, these commenters recommended that bank service providers should work with their banking organizations to designate a central point of contact, but bank service providers should not be required to ensure that a contact at the banking organization receive the notification.[51]

Regarding existing provisions in contracts, a commenter contended that "contractual provisions with bank service providers commonly provide specific notice methods and generally provide notice to two or more banking organization employees." This is consistent with the agencies' understandings of existing agreements based on their broad-based review of bank service provider agreements, which was reflected in the language of the proposed rule.

As an alternative to the approach in the proposed rule, a few commenters suggested that the rule should "instead focus on outcomes—ensuring that the appropriate individuals or entities at banking organizations receive timely notice." Another commenter suggested that "banking organizations should have a central point of contact that would be accessible by more than one person to ensure that notifications to the banking organization are timely received and acted upon." This approach was echoed by another banking industry commenter, who suggested that

[50] Commenters suggested that one contact should be adequate, as smaller banking organizations may not have two contacts available.

[51] A commenter also recommended different notification obligations for on-premises services compared to cloud-based services. Commenters also suggested a carve-out to the notification obligation when a bank service provider is delayed or prevented by law enforcement.

"notification through a medium or channel that is accessed by and available to multiple banking organization employees" should be allowed to meet the NPR's notification requirement. Some commenters suggested using automated notifications or centralized notification portals to streamline the notification process.

After consideration of the comments, the agencies are revising the final rule to keep the notification process simple and flexible. Rather than requiring bank service providers to notify two individuals at each affected banking organization customer, which may not be effective for every banking organization or bank service provider, the final rule requires bank service providers to notify "at least one bank-designated point of contact at each affected banking organization customer." The final rule states that a banking organization-designated point of contact is an email, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer.

The agencies determined effective notice will be best achieved if banking organizations and bank service providers work collaboratively to designate a method of communication that is feasible for both parties and reasonably designed to ensure that banking organizations actually receive the notice in a timely manner. The final rule also provides flexibility for banking organizations and bank service providers to determine the appropriate designated point of contact, and if a banking organization customer has not previously provided a bank-designated point of contact, such notification shall be made to the Chief Executive Officer (CEO) and Chief Information Officer (CIO) of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means.

iv. Bank Service Provider Agreements - Contract Notice Provisions

Several commenters observed that contracts between banking organizations and bank service providers routinely include incident notification provisions.[52] But other commenters noted that current contractual provisions may not align with the proposed rule's notification requirements and, as such, would need to be amended or revised, which may take time to complete.

Commenters generally stated that while contracts between banking organizations and bank service providers already have negotiated notice provisions, such contracts would need to be amended to ensure compliance with the rule. In that regard, commenters expressed the view that the proposed rule should be revised to allow for bank service providers to satisfy their notification requirement by providing notification to their banking organization customer consistent with any requirements and by any methods set forth in their contract with that customer, so long as the method reasonably ensures that the banking organization customer receives the notification. Facilitating compliance with the rule in this manner would prevent banking organizations from having to incur the costs to amend existing contracts. Other commenters expressed perceived challenges with renegotiating contracts to comply with the rule and commenters stated that they should not be faulted for a bank service provider's failure to notify. One commenter expressed concern that community banks may hold little power in these negotiations and recommended extending the compliance date of the rule for community banks. Relatedly, a commenter argued that if FMUs are required to provide mandated notices to their banking organization customers, the rule should require banking organization customers to

[52] A commenter stated that bank service providers already subject to contractual breach reporting obligations should be excluded from the rule while a different commenter believed that as a matter of fairness and competitive equality, if private sector FMUs are required to provide mandated notices to either their primary federal regulator or their banking organization customers, the Board should publicly commit to hold Federal Reserve Bank services to an equivalent standard.

identify and update their contacts for mandated notices to their bank service providers, rather than placing the burden on bank service providers to request and seek updates to these contacts. Commenters also urged the agencies to accept the notification methods specified in these contracts and clarify contract expectations. A few commenters requested that the agencies provide specific contract expectations and to consider conducting a review of contracts to confirm the notice provisions were adequate.

The agencies believe many contracts already address such notices to banking organizations. 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. If such notification provisions satisfy the requirements of the final rule, then notification under the contractual provisions will satisfy a bank service provider's obligation under the rule as well. The agencies note that existing notification procedures may include some redundancy with the final rule. However, the agencies are requiring notice in the final rule to ensure that a notification occurs in the event of a material computer-security incident. As a result, the agencies are not incorporating these recommendations. The agencies also note that the notification requirement created by this rule is independent of any contractual provisions, and therefore, bank service providers must comply even where their contractual obligations differ from the notification requirement in this rule. The agencies anticipate that banking organizations and bank service providers will work collaboratively to designate a method of communication that is feasible for both parties and reasonably designed to ensure that banking organizations actually receive the notice in a timely manner, for purposes of complying with the rule.

This final rule is not expected to add significant burden on bank service providers. The

agencies' experiences with conducting bank service provider contract reviews during examinations indicate that many of these contracts include incident-reporting provisions. The agencies also observe that there are effective automated systems for notification currently.

In addition, for banking organizations that have not already designated individuals to be notified under contractual obligations, the agencies do not believe that requiring bank service providers to notify banking organization CEOs and CIOs would create significant burden. In these circumstances, the agencies believe that bank service providers can easily obtain contact information for banking organization CEOs and CIOs.

IV. Other Rulemaking Considerations

In the NPR, the agencies sought feedback on a number of related topics, which are addressed separately in the sections that follow.

A. Bank Service Provider Material Incidents Consideration

The agencies requested comments about the potential burden the rule would impose on small bank service providers and about circumstances when a banking organization customer would not be aware of a material disruption in services unless they were notified. There were limited comments on this question.

A few commenters noted that banking organizations are often contacted by their customers shortly after an incident and service outage occurs. Despite indirect knowledge or suspicions about potential service outages or limitations, banking organizations should still be notified of material incidents by their bank service providers.

Merely identifying the fact of an outage or service interruption would not help banking organization customers understand the extent of such an outage or service interruption. Receiving notification from a bank service provider would enable a banking organization

customer to evaluate the impact of the computer-security incident on its operations to determine whether it is experiencing a notification incident. If a banking organization is experiencing a notification incident and notifies its primary federal regulator, the regulator then may evaluate and assist, as appropriate.

B. Methodology for Determining Number of Incidents Subject to the Rule

The agencies invited comment on the methodology used to estimate the number of notification incidents that may be subject to the proposed rule each year. Several commenters provided general comments suggesting the agencies may have underestimated the burden associated with the proposed rule; however, only one trade association commenter provided specific observations on the methodology used to estimate the number of incidents subject to the rule. This commenter suggested that the agencies should "seek additional comments on the estimated costs and benefits of the proposed rule."

The agencies also received comments related to the costs associated with complying with the rule. A commenter asserted, without further detail, that the proposed costs of compliance were underestimated. This commenter suggested that the agencies gather more information and data to adequately assess the regulatory impact of the proposal. Regarding estimating the number of notification incidents per year that would be reported under the proposed rule, one commenter suggested the agencies already have this information. Another commenter asserted that the rule would result in significant costs in standing up internal processes and procedures to comply with a new federal regulatory mandate, resulting in ongoing cost and burden.

The agencies have addressed the costs of this rule in the Impact Analysis section below. Moreover, the methodology used to determine the number of incidents subject to the rule reflects the agencies' experience that computer-security incidents that rise to the level of notification

incidents are rare. The agencies also believe that the final rule largely formalizes a process that already exists, reflecting the collaborative and open communication that exists between banking organizations and the agencies.

As discussed in more detail in the Impact Analysis section, the agencies reviewed available supervisory data and a subset of Suspicious Activity Report (SAR) data involving cyber incidents targeting banking organizations to develop an estimate of the number of notification incidents that may occur annually. The agencies specifically recognized that an analysis of SAR filings would not capture the full scope of incidents addressed by this rule. However, the agencies also considered supervisory data, which includes the voluntary notification banking organizations already provide, to inform their estimate of the frequency of notification incidents. Based on this assessment, the agencies continue to believe that the estimated 150 notification incidents annually set forth in the Impact Analysis is reasonable. The agencies are not seeking additional comments on the estimated costs and benefits of the rule.

C. Voluntary Information Sharing

One commenter suggested the agencies should acknowledge the importance of voluntary information sharing within an "expanding notice schema," and rely upon voluntary disclosures for non-disruptive events. Another suggested the rule should "distinguish between existing, voluntary information-sharing between banking organizations" and the final rule's required incident notification disclosures.

The focus and purpose of this final rule is to ensure that the agencies receive prompt notice of notification incidents, which we have defined to include only the most significant incidents affecting banking organizations. The final rule does not solicit notifications on non-disruptive events and differs from and does not prevent traditional supervisory information

sharing. However, the agencies agree that voluntary information sharing is critically important and encourage banking organizations and bank service providers to continue sharing information about incidents not covered by this rule.

D. Utilizing Prompt Corrective Action Capital Classifications

One commenter suggested incorporating "existing terms and definitions of discrete, rare, disruptive events" such as "Prompt Corrective Action (PCA) capital category definitions, or the invocation of Sheltered Harbor protocols."[53] The agencies decline to follow this recommendation. The agencies have used definitions in the final rule that are broadly consistent with NIST terminology, which is widely used across various industry segments.

E. Ability to Rescind Notification and Obtain Record of Notice

The agencies received several comments regarding the agencies' collection and use of notification incident information from banking organizations. One commenter urged the agencies to develop procedures, subject to notice and comment, that would be taken upon receipt of a banking organization's incident notification information and any subsequently gathered information related to the incident. Commenters also urged the agencies to clarify information sharing practices and protocols relating to notification incident reports, expressing concerns with confidentiality and data security. One commenter suggested that notification incident reports should be shared with banking organization-specific supervisory teams. Commenters stated that any information submitted should be subject to the agencies' confidentiality rules and that the agencies should explain how the information would be protected.

One commenter suggested the agencies establish a "mechanism to rescind" notifications

[53] To learn more about PCA capital category definitions, see OCC Bulletin 2018-33, *Prompt Corrective Action: Guidelines and Rescissions* (Sept. 28, 2018), which can be found at: *https://www.occ.gov/news-issuances/bulletins/2018/bulletin-2018-33.html*. To learn more about Sheltered Harbor protocols, see the Sheltered Harbor landing page at: *https://www.aba.com/banking-topics/technology/cybersecurity/sheltered-harbor#.*

in situations where "initial determinations overestimate[d] the severity or significance of an event." No formal rescission mechanism is required. The agencies recognize that a banking organization or bank service provider may provide notice, from time to time, upon a mistaken determination that such notice is necessary. A banking organization or bank service provider may update its original notification if it later determines that its initial assessments were incorrect or overcautious.

Other commenters discussed the need to obtain or retain copies of the notifications for recordkeeping purposes. The rule does not impose any recordkeeping requirements.

Another commenter suggested the agencies should indicate how information that the agencies obtain under this rule would remain protected and confidential. Additionally, they requested confirmation that the information provided would be considered exempt from Freedom of Information Act (FOIA) requests. As the agencies noted in the proposal, the notification, and any information provided by a banking organization related to the incident, would be subject to the agencies' confidentiality rules, which provide protections for confidential, proprietary, examination/supervisory, and sensitive personally identifiable information.[54] However, the agencies must respond to individual FOIA requests on a case-by-case basis.

F. Single Notification Definition

One commenter suggested the agencies implement only a "single definition for a notification incident that applies to both bank service providers and banking organizations." The agencies believe that this would be unworkable; the two notification requirements serve different purposes. Accordingly, the agencies declined to implement a single definition. However, the agencies have sought to harmonize the two notification standards where feasible.

[54] *See, e.g.*, 12 CFR part 4 (OCC); 12 CFR part 261 (Rules Regarding Availability of Information) (Board); 12 CFR 309.6 (Disclosure of exempt records) (FDIC).

G. Affiliated Banking Organizations Considerations

The final rule provides that affiliated banking organizations each have separate and independent notification obligations. Each banking organization needs to make an assessment of whether it has suffered a notification incident about which it must notify its primary federal regulator. Subsidiaries of banking organizations that are not themselves banking organizations do not have notification requirements under this final rule. If a computer-security incident were to occur at a non-banking organization subsidiary of a banking organization, the parent banking organization would need to assess whether the incident was a notification incident for it, and if so, it would be required to notify its primary federal regulator.

H. Consideration of the Number of Bank Service Providers

Some commenters suggested the agencies underestimated the impact of the NPR to bank service providers. As noted in the NPR, the agencies do not know the precise number of bank service providers that will be affected by the final rule's notification requirement. However, the agencies conservatively assumed the entire population of bank service providers who 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 to be the estimated number of bank service providers. It seems unlikely that all such code 5415-designated firms are bank service providers. Even though there may be some bank service providers that do not self-identify under NAICS code 5415, the agencies believe the number of incidents involving bank service providers will be generally consistent with original NPR findings. The agencies acknowledge that these bank service providers will be impacted by the final rule.

V. Impact Analysis

Covered banking organizations under the final rule include all depository institutions, holding companies, and certain other financial entities that are supervised by one or more 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 are covered under the final rule.[55]

In addition, the final rule requires bank service providers to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. 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.

Benefits

The agencies believe that prompt notification of reportable incidents is likely to provide the following benefits to banking organizations and the financial industry as a whole. Notification may help the relevant agencies determine whether the incident is isolated or is one of many 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 on behalf of the affected organization to minimize the impact of the incident. This benefit may be greater for small banking organizations with more limited resources. If the notification incident is one of many similar incidents occurring at multiple

[55] March 31, 2021, Call Report Data.

banking organizations, the agencies could also alert other banking organizations of the threat, recommend measures to better manage or prevent the recurrence of similar incidents, or otherwise help coordinate incident response.

The prompt notification about incidents could also enable federal regulators to respond faster to potential liquidity events that may result from such incidents. If a notification incident prevents banking organizations from fulfilling financial obligations in a timely manner, it might reduce confidence in the banking organization and precipitate the rapid withdrawal of demand deposits or short-term financing from such organizations.[56,57] The agencies believe that a faster regulatory response could mitigate, or entirely prevent, these adverse liquidity events, thereby enhancing the resilience of the banking system against notification incidents.

Receiving information on notification incidents at multiple banking organizations would also enable regulators to conduct empirical analyses to improve related guidance, adjust supervisory programs to enhance resilience against such incidents, and provide information to the industry to help banking organizations reduce the risk of future computer-security incidents.

The agencies do not have sufficient information available to quantify the potential benefits of the final rule because the benefits depend on the probability, breadth, and severity of future notification incidents, and the specifics of those incidents, among other things. These data limitations notwithstanding, and considering that banking organizations face a heightened risk of disruptive and destructive attacks, which have been increasing in frequency and severity in recent years, the agencies expect that the final rule would have clear prudential benefits.

[56] See the conceptual discussion of "cyber runs" in Duffie and Younger, *https://www.brookings.edu/wp-content/uploads/2019/06/WP51-Duffie-Younger-2.pdf*, Hutchins Center Working Paper No. 51, June 18, 2019.
[57] See the empirical analysis of the potential adverse impact of cyber events on the U.S. payment and settlement system in Eisenbach et al., *https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr909.pdf,* Federal Reserve Bank of New York Staff Reports, No. 909, Last Revised May 2021.

Costs

The final rule requires 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 in 2019 and 2020 to estimate the number of notification incidents expected to be reported annually. This calculation relied on descriptive criteria (e.g., ransomware, trojan, zero day, etc.) that may be indicative of the type of material computer-security incident that would meet the notification incident reporting criteria. Based on this review, the agencies estimate that approximately 150 notification incidents occurred annually,[58] but acknowledge that the number of such incidents could increase in the future. Comments received by the agencies on the NPR did not provide more accurate estimates or suggest a different estimation methodology. Therefore, the agencies continue to use the same methodology.

The agencies believe that the regulatory burden associated with the notification requirement would be small because the majority of communications associated with the determination of the notification incident would occur regardless of the final rule.[59] In particular, the agencies estimate that, in the event of a notification incident, an affected banking organization may incur up to three hours of labor cost to coordinate internal communications, consult with its bank service provider, if appropriate, and notify the banking organization's primary federal regulator. This process may include discussion of the incident among staff of the

[58] 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.

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

banking organization, such as the Chief Information Officer, 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 final rule also requires a bank service provider to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. The agencies do not have data on the exact number of affected bank service providers nor the frequency of incidents that would require bank service providers to notify their banking organization customers. However, as described in the NPR, the agencies believe that, in the event of an incident, the affected bank service provider may incur up to three hours of labor cost to coordinate internal communications and notify its affected banking organization customers. Commenters did not provide other estimates, and the agencies believe that the additional compliance costs would be small for individual affected bank service providers.[60] Post-notification activities, such as providing technical support to affected bank organization customers when managing and resolving the impact of a computer-security incident, are beyond the scope of the notification requirement.

Overall, the agencies expect the benefits of the final rule to outweigh its small costs.

Response to comments on impact of proposal

The agencies received comments asserting that some banking organizations and bank service providers may need to revise their contracts in order to implement the final rule. Furthermore, some bank service providers may incur costs to adjust internal processes and

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

procedures to comply with the final rule. The agencies believe that these costs are likely to be small, transitory, and affect only a small number of covered entities.

Other comments received in response to the proposed rule suggested that the proposed rule's definitions might result in more notifications than estimated in the proposed rule. The final rule narrows the notification requirements, as discussed above.

VI. Alternatives Considered

The agencies are adopting these computer-security incident notification requirements after considering comments received on the NPR and evaluating alternative options for notification requirements. The agencies considered a number of alternative approaches, including leaving the current regulations unchanged and establishing a voluntary notification framework as suggested by one commenter. The agencies concluded that these approaches would not have achieved the objectives of the rule. However, the agencies refined the criteria for notification to focus attention on the most significant incidents and appropriately minimize regulatory burden.

Additionally, the agencies considered defining the notification requirement for bank service providers even more narrowly, as suggested by some commenters. However, the agencies ultimately determined that the notification requirement in this rule is appropriate due to the increasingly significant role that bank service providers play in the banking industry.

VII. Effective Date

The agencies have provided an effective date of April 1, 2022, and a compliance date of May 1, 2022, in response to commenters that recommended that the agencies provide additional time to implement the rule.

VIII. Administrative Law Matters

A. Paperwork Reduction Act

Certain provisions of the final rule contain "collections of information" 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 have requested and OMB has assigned to the agencies the respective control numbers shown. The information collections contained in the final rule 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 § 1320.11 of OMB's implementing regulations (5 CFR part 1320). The Board reviewed the final rule under the authority delegated to the Board by OMB, and has approved these collections of information.

The final rule contains a reporting requirement that is subject to the PRA. The reporting requirement is found in §§ 53.3 (OCC), 225.302 (Board), and 304.23 (FDIC) of the final rule. A banking organization is required to notify its primary federal bank regulatory agency of the occurrence of a "notification incident" at the banking organization (§§ 53.3 (OCC), 225.302 (Board), and 304.23 (FDIC)).

The final rule also contains a disclosure requirement that is subject to the PRA. The disclosure requirement is found in §§ 53.4 (OCC), 225.303 (Board), and 304.24 (FDIC), which requires a bank service provider to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

The agencies received one PRA-related comment, which agreed that collections of information have practical utility.

The agencies have a continuing interest in the public's opinions of information collections. At any time, commenters may submit comments regarding the burden estimate, or any other aspect of this collection of information, including suggestions for reducing the burden, to the addresses listed in the ADDRESSES caption in the NPR. All comments will become a matter of public record. 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; by facsimile to (202) 395– 5806; or by email to: oira_submission@ omb.eop.gov, Attention, Federal Banking Agency Desk Officer.

Proposed Information Collection

Title of Information Collection: Computer-Security Incident Notification.

OMB Control Number: OCC 1557-0350; Board 7100-NEW; FDIC 3064-0214.

Frequency of Response: On occasion; event-generated[61]

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, insured State savings associations, and bank service providers.

Board: All state member banks (as defined in 12 CFR 208.2(g)), bank holding companies (as defined in 12 U.S.C. 1841), savings and loan holding companies (as defined in 12 U.S.C. 1467a),

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

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[62]*:*

OCC: Reporting – 22; Disclosure – 802.

FDIC: Reporting – 96; Disclosure – 802.

Board: Reporting – 32; Disclosure – 802.

Estimated Hours per Response:

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

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

Estimated Total Annual Burden:

OCC: Reporting – 66 hours; Disclosure – 2,406 hours.

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

Board: Reporting – 96 hours; Disclosure – 2,406 hours.

Abstract: The final rule establishes notification requirements for banking organizations upon the occurrence of a "computer-security incident" that rises to the level of a "notification incident." A "notification incident" is defined as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's—

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

(i) ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

(ii) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

(iii) operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

A "computer-security incident" is defined as is an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

The final rule requires 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 final rule imposes a limited amount of burden, beyond what is usual and customary, on banking organizations in the event of a computer-security incident even if it does not rise to the level of a notification incident, as banking organizations will need to 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 incidents.

The final rule also requires a bank service provider to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered

services provided to such banking organization for four or more hours.

B. Regulatory Flexibility Act

OCC: The Regulatory Flexibility Act (RFA), 5 U.S.C. 601 *et seq.*, requires an agency, in connection with a final rule, to prepare a Final 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 final rule will not have a significant economic impact on a substantial number of small entities. The OCC currently supervises approximately 669 small entities.

Because the final rule impacts all OCC-supervised institutions, as well as all bank service providers, it will impact a substantial number of small entities. However, the expected costs of the final rule will 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 final rule. 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 final rule will not have a significant economic impact on a substantial number of small entities.

Board: The Regulatory Flexibility Act (RFA) generally requires an agency, in connection with a final rule, to prepare and make available for public comment a final regulatory flexibility analysis that describes the impact of the rule on small entities.[63] However, a regulatory

[63] 5 U.S.C. 601 *et seq.*

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. For the reasons described below, the Board certifies that the final rule will not have a significant economic impact on a substantial number of small entities.

As discussed in the **Supplementary Information** section, the agencies are requiring a banking organization to notify its primary federal regulator as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule will establish a notification requirement, which would support the safety and soundness of entities supervised by the agencies. The final rule requires a bank service provider, as defined in the rule, to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

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, and Edge and agreement corporations (collectively, "Board-regulated entities"). As described in the Impact Analysis section, requirements under the final rule will apply to all Board-regulated entities. Under regulations issued by the SBA, a small entity includes a depository institution, bank 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.[64] According to Call Reports and other Board reports, there were

[64] As an example, the SBA defines a bank as small if it has $600 million or less in assets. *See* 13 CFR 121.201 (as

approximately 451 state member banks, 2,380 bank holding companies, 92 savings and loan holding companies, and 16 Edge and agreement corporations that are small entities.[65] In addition, the final rule affects all bank service providers that provide services subject to the BSCA.[66] 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 final rule will require all banking organizations to notify the appropriate Board-designated point of contact about a notification incident through email, telephone, or other similar methods that the Board may prescribe. The Board must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. 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 final rule.

The final rule will also require a bank service provider to notify at least one bank-

---

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.

[65] State member bank data is derived from June 30, 2021 Call Reports. Data for bank holding companies and savings and loan holding companies are derived from the June 30, 2021, FR Y-9C and FR Y-9SP. Data for Edge and agreement corporations are derived from the December 31, 2020, FR-2886b.

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

designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. 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 final rule.

For the reasons stated above, the Board certifies that the final rule will not have a significant economic impact on a substantial number of small entities.

FDIC: The RFA generally requires an agency, in connection with a final rule, to prepare and make available for public comment a final regulatory flexibility analysis that describes the impact of the rule on small entities.[67] 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 SBA has defined "small entities" to include banking organizations with total assets of less than or equal to $600 million.[68] 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

[67] 5 U.S.C. 601 *et seq.*

[68] 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.

institutions. For the reasons described below, the FDIC certifies that the final rule will not have a significant economic impact on a substantial number of small entities.

As described in the Impact Analysis section, the final rule is expected to affect all institutions supervised by the FDIC. According to recent Call Reports, the FDIC supervises 3,215 insured depository institutions (FDIC-supervised IDIs).[69] Of these, 2,333 FDIC-supervised IDIs would be considered small entities for the purposes of RFA.[70] These small entities hold approximately $510 billion in assets, accounting for 13 percent of total assets held by FDIC-supervised institutions. In addition, the final rule affects all bank service providers that provide services subject to the BSCA.[71] 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.

The final rule requires a banking organization to notify the appropriate FDIC supervisory office, or an FDIC-designated point of contact, about a notification incident through email, telephone, or other similar methods that the FDIC may prescribe. The FDIC must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. 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

[69] FDIC Call Reports, March 31, 2021
[70] *Id.*
[71] Discussed in detail in the Impact Analysis section.

notification incident would have occurred regardless of the final rule.[72]

In addition, the final rule will require a bank service provider to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours. 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.

Therefore, the FDIC certifies that the final rule will not have a significant economic impact on a substantial number of small entities.

C. Riegle Community Development and Regulatory Improvement Act of 1994

Under section 302(a) of the Riegle Community Development and Regulatory Improvement Act (RCDRIA),[73] in determining the effective date and administrative compliance requirements for new regulations that impose additional reporting, disclosure, or other requirements on insured depository institutions (IDIs), each Federal banking agency must 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, section 302(b) of RCDRIA requires new regulations and amendments to regulations that impose additional reporting, disclosures, or other new requirements on IDIs generally to take effect on the first day of a calendar quarter that begins on

[72] Even at an elevated labor compensation rate of $200 per hour, the final rule would impose a cost burden of less than $600 per incident.
[73] 12 U.S.C. 4802(a).

or after the date on which the regulations are published in final form.[74] The agencies have determined that the final rule would impose additional reporting, disclosure, or other new requirements on IDIs, and are making this final rule effective in accordance with the requirements of the RCDRIA.

D. Congressional Review Act

For purposes of the Congressional Review Act (CRA), the Office of Management and Budget (OMB) makes a determination as to whether a final rule constitutes a "major rule."[75] If a rule is deemed a "major rule" by the OMB, the CRA generally provides that the rule may not take effect until at least 60 days following its publication.[76] The Congressional Review Act defines a "major rule" as any rule that the Administrator of the Office of Information and Regulatory Affairs of the OMB finds has resulted in or is likely to result in—(A) an annual effect on the economy of $100,000,000 or more; (B) a major increase in costs or prices for consumers, individual industries, Federal, State, or Local government agencies or geographic regions, or (C) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets.[77]

The agencies will submit the final rule to the OMB for this major rule determination. As required by the Congressional Review Act, the agencies will also submit the final rule and other appropriate reports to Congress and the Government Accountability Office for review.

E. Use of Plain Language

---

[74] *Id*. at 4802(b).
[75] 5 U.S.C. 801 *et seq*.
[76] 5 U.S.C. 801(a)(3).
[77] 5 U.S.C. 804(2).

Section 722 of the Gramm-Leach-Bliley Act[78] requires the Federal banking agencies to use plain language in all proposed and final rulemakings published in the *Federal Register* after January 1, 2000. The agencies invited comment regarding the use of plain language, but did not receive any comments on this topic.

F. Unfunded Mandates Reform Act

The OCC analyzed the final 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 final 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 $158 million). As noted in the OCC's RFA discussion, the OCC expects that the costs associated with the final rule, if any, will be *de minimis* and, thus, has determined that this final rule will not result in expenditures by State, local, and Tribal governments, or the private sector, of $158 million or more in any one year. Accordingly, the OCC has not prepared a written statement to accompany this final rule.

IX. Agency Regulation

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

[78] 12 U.S.C. 4809.

Administrative practice and procedure, Bank holding companies, banking, Edge and agreement corporations, Foreign banking organizations, Nonbank financial companies, 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, Freedom of information, Reporting and recordkeeping requirements, Safety and soundness.

Authority and Issuance – OCC

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 amends 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 computer-security incidents that may materially and adversely affect OCC-supervised institutions.

(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 their bank service providers as defined in § 53.2(b)(2).

§ 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 subpart, the following definitions apply.

(1) *Banking organization* means a national bank, Federal savings association, or Federal branch or agency of a foreign bank; provided, however, that no designated financial market utility shall be considered a banking organization.

(2) *Bank service provider* means a bank service company or other person that performs covered services; provided, however, that no designated financial market utility shall be considered a bank service provider.

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

(4) *Computer-security incident* is an occurrence that results in actual harm to the

confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

(5) *Covered services* are services performed, by a person, that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867).

(6) *Designated financial market utility* has the same meaning as set forth at 12 U.S.C. 5462(4).

(7) *Notification incident* is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's—

(i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

(ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

(iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

(8) *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 appropriate OCC supervisory office, or OCC-designated point of contact, about a notification incident through email, telephone, or other similar methods

that the OCC may prescribe. The OCC must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred.

§ 53.4 Bank service provider notification.

(a) A bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

(1) A bank-designated point of contact is an email address, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer.

(2) If the banking organization customer has not previously provided a bank-designated point of contact, such notification shall be made to the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means.

(b) The notification requirement in paragraph (a) of this section does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer.

FEDERAL RESERVE SYSTEM

12 CFR Chapter II

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, and 3101 *et seq.*, the Board amends chapter II of Title 12, Code of Federal Regulations, as follows:

PART 225—BANK HOLDING COMPANIES AND CHANGE IN BANK CONTROL (REGULATION Y)

2. The authority citation for part 225 continues to read as follows:

Authority: 12 U.S.C. 1817(j)(13), 1818, 1828(o), 1831i, 1831p-1, 1843(c)(8), 1844(b), 1972(1), 3106, 3108, 3310, 3331-3351, 3906, 3907, and 3909; 15 U.S.C. 1681s, 1681w, 6801, and 6805.

3. Subpart N is added to read as follows:

Subpart N—Computer-Security Incident Notification

Sec.

Subpart N—Computer-Security Incident Notification

§ 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, and 3101 *et seq*.

(b) *Purpose.* This subpart promotes the timely notification of computer-security incidents that may materially and adversely affect Board-supervised entities.

(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 their

bank service providers, as defined in § 225.301(b)(2).

§ 225.301 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 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 or agreement corporation; provided, however, that no designated financial market utility shall be considered a banking organization.

(2) *Bank service provider* means a bank service company or other person that performs covered services; provided, however, that no designated financial market utility shall be considered a bank service provider.

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

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

(5) *Covered services* are services performed, by a person, that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867).

(6) *Designated financial market utility* has the same meaning as set forth at 12 U.S.C. 5462(4).

(7) *Notification incident* is a computer-security incident that has materially

disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's—

(i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

(ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

(iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

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

§ 225.302 Notification.

A banking organization must notify the appropriate Board-designated point of contact about a notification incident through email, telephone, or other similar methods that the Board may prescribe. The Board must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred.

§ 225.303 Bank service provider notification.

(a) A bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has

materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

(i) A bank-designated point of contact is an email address, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer.

(ii) If the banking organization customer has not previously provided a bank-designated point of contact, such notification shall be made to the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means.

(b) The notification requirement in paragraph (a) of this section does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer.

FEDERAL DEPOSIT INSURANCE CORPORATION

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 amends 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, 1811, 1813, 1817, 1819, 1831, and 1861–1867.

2. Revise § 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.

§§ 304.15–304.20 [Reserved]

3. Reserve §§ 304.15 through 304.20.

4. Add subpart C to read as follows:

Subpart C - Computer-Security Incident Notification

Sec.

304.21 Authority, purpose, and scope.

304.22 Definitions.

304.23 Notification.

304.24 Bank service provider notification.

SUBPART C - COMPUTER-SECURITY INCIDENT NOTIFICATION

§ 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 computer-security incidents that may materially and adversely affect FDIC-supervised institutions.

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

§ 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 insured State savings associations; provided, however, that no designated financial market utility shall be considered a banking organization.

(2) *Bank service provider* means a bank service company or other person that performs covered services; provided, however, that no designated financial market utility shall be considered a bank service provider.

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

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

(5) *Covered services* are services performed, by a person, that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867).

(6) *Designated financial market utility* has the same meaning as set forth at 12 U.S.C. 5462(4).

(7) *Notification incident* is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's—

(i) Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;

(ii) Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or

(iii) Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

(8) *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 appropriate FDIC supervisory office, or an FDIC-designated point of contact, about a notification incident through email, telephone, or other similar methods that the FDIC may prescribe. The FDIC must receive this notification from the banking organization as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred.

§ 304.24 Bank service provider notification.

(a) A bank service provider is required to notify at least one bank-designated point of contact at each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours.

(1) A bank-designated point of contact is an email address, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer.

(2) If the banking organization customer has not previously provided a bank-designated point of contact, such notification shall be made to the Chief Executive Officer and Chief Information Officer of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means.

(b) The notification requirement in paragraph (a) of this section does not apply to any scheduled maintenance, testing, or software update previously communicated to a banking organization customer.

§§ 304.25–304.30 [Reserved]

5. Reserve §§ 304.25 through 304.30.

Michael J. Hsu,

Acting Comptroller of the Currency.

By order of the Board of Governors of the Federal Reserve System.

Ann Misback,

Secretary of the Board.

Federal Deposit Insurance Corporation.

By order of the Board of Directors.

Dated at Washington, DC, on October __, 2021.

James P. Sheesley,

Assistant Executive Secretary.

[**BILLING CODE**S: 4810-33-P; 6210-01-P; 6714-01-P]