Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990 Division of Risk Management Supervision

MEMORANDUM TO: Board of Directors

FROM: Doreen R. Eberley
Director, Division of Risk Management Supervision

SUBJECT: Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers

RECOMMENDATION

Staff is presenting for consideration by the FDIC Board of Directors ("Board") the attached final rule requiring notification to federal regulators and banking organization[1] customers following certain material computer-security incidents.

SUMMARY

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the Office of the Comptroller of the Currency (OCC) (collectively, "the Agencies"), have drafted a final rule that would require 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. Additionally, under the final rule, third-party bank service providers must notify banking organization customers as soon as possible whenever a provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to disrupt or degrade, for four or more hours, the performance of services subject to the Bank Service Company Act (BSCA)[2] that are provided to such banking organizations.

CONCUR:

Nicholas J. Podsiadly
General Counsel

[1] The final rule defines "Banking organization" as "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] 12 U.S.C. §§ 1861–1867.

Notification by Banks to Federal Regulators

As defined in the final rule, a "notification incident" is a computer-security incident[3] 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.

Notification by Third Party Providers to Banking Organization Customers

Bank service providers must notify at least one bank-designated point of contact[4] at each affected banking organization customer "as soon as possible" after the bank service provider has determined it has experienced a computer-security incident that "has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade," BSCA-covered services for four or more hours. The final rule exempts scheduled maintenance from the requirement.

EXISTING REPORTING REQUIREMENTS

There is no general federal requirement that banking organizations promptly notify their financial regulators of a computer-security incident that may materially disrupt a banking organization's operations or negatively impact its financial condition. The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,[5] which interprets section 501(b) of the Gramm- Leach-Bliley Act (GLBA),[6] provides that financial institutions have response program procedures to notify their primary federal regulator "as soon as possible" when an institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.[7] While this provides for prompt federal regulator notice of certain computer-security incidents, this requirement is narrow in scope and does not capture operational incidents that do not involve compromised customer information.

Additional incidents are reported under part 353 of the FDIC's rules and regulations through suspicious activity reports (SAR); however, the filing of a SAR may not take place for up to 60

---

[3] The final rule defines "computer-security incident" as "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."
[4] The final rule defines "bank-designated point of contact" as "an email address, phone number, or any other contact(s), previously provided to the bank service provider by the banking organization customer."
[5] *See* 12 C.F.R. § 364 app'x B, supp. A (FDIC) ("Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice").
[6] *See* Pub. L. No. 106-102, § 501, 113 Stat. 1436 (1999) (codified at 15 U.S.C. § 6801).
[7] *See* 12 C.F.R. § 364 app'x B, supp. A.

calendar days from the time that the suspicious activity has been identified.[8] The information from SARs is not timely enough for the Agencies to provide support to a financial institution, or more broadly, to allow the Agencies to identify emergent risks that may challenge the financial sector.

The final rule seeks to close this reporting gap. Earlier notification from every affected banking organization would allow the Agencies to assess the severity and spread of disruptive computer-security incidents. The Agencies could then take appropriate actions, including alerting other banking organizations, consulting with security and law enforcement agencies, and assisting in coordinating a response. These actions could mitigate the impact of the incident and help preserve the safety and soundness of the financial industry. The FDIC may also become aware at an earlier point in time of extreme cases that may threaten the viability of a particular institution.

NOTICE OF PROPOSED RULEMAKING

On January 12, 2021, the Agencies published in the Federal Register a Notice of Proposed Rulemaking (NPR) seeking comments on a proposed regulation requiring notifications from banking organizations and their bank service providers following computer-security incidents rising to a certain level of severity. The NPR proposed to establish a new subpart C in part 304 of the FDIC's regulations (12 C.F.R. §§ 304.21–304.24) titled "Computer-Security Incident Notification." The FRB and OCC promulgated similar proposed rules. The NPR presented 16 specific questions for commenters to consider and invited comment on all other aspects of the proposed rule.[9]

A. Computer-Security Incident and Notification Incident Defined

The NPR defined two key terms as part of the rulemaking: "computer-security incident" and "notification incident." For the NPR's proposed definition of "computer-security incident," the Agencies adopted the principal definition employed by the National Institute of Standards and Technology (NIST).[10] "Notification incident" further narrowed reportable computer-security incidents to the following:[11]

> [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;

[8] *See* 12 C.F.R. § 353.3(b), (1)-(2).

[9] The comment period ended on April 12, 2021.

[10] The proposed definition was, "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."

[11] 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 FRB and FDIC under section 165(d) of the Dodd-Frank Act. The Agencies do not expect banking organizations that are not subject to the Resolution Planning Rule to identify "core business lines" or "critical operations," or to develop procedures to determine whether they engage in any operations the failure or discontinuance of which would pose a threat to the financial stability of the United States.

(ii) any business line of a banking organization, including associated operations, services, functions, and support, and would result in a material loss of revenue, profit, or franchise value; or

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

B. Reporting of Incidents

The NPR established notification requirements for two types of entities. First, the Agencies proposed to require a banking organization to provide its primary federal regulator with prompt notification of any "computer-security incident" that rises to the level of a "notification incident." The proposed rule would have required such notification upon the occurrence of a notification incident as soon as possible and no later than 36 hours after the banking organization "believes in good faith that the incident occurred." This notification was intended to serve as an early alert to a banking organization's primary federal regulator, and was not intended to require comprehensive or elaborate reporting.

Second, the NPR also would have required a bank service provider to notify at least two individuals at affected banking organization customers "immediately" after the bank service provider experienced a computer-security incident that it believed "in good faith" could "disrupt, degrade, or impair" services provided for four or more hours.

DISCUSSION OF COMMENTS

In response to the NPR, the Agencies collectively received 35 comment letters, some with multiple organizations as signatories. The commenters included trade associations representing banks and major technology companies, banks, technology service providers, retail payment card networks, and others.

Commenters generally agreed that banking organizations should notify the Agencies when they experience a computer-security incident that materially disrupts their ability to provide core banking services or results in a material financial loss. There was, however, a wide variety of observations on whether and how such notification should be codified, with several suggested modifications. Four commenters opposed the proposal, contending that compliance would be burdensome or duplicative of existing requirements, and might impede banking organizations' and bank service providers' abilities to respond effectively to incidents.

Some commenters suggested that financial market utilities be excluded from the definition of "banking organization." A few commenters suggested clarifying that the rule only applied to service providers providing services that are subject to the BSCA. Some suggested that the final rule should include additional third-party entities (e.g., Fintech firms).

A frequent theme was a desire for clarification of "computer-security incident" and "notification incident." Commenters generally supported adoption of NIST's definition for "computer-security incident" in principle, but noted that NIST's definition was overly broad given the purpose of the regulation. Specifically, commenters suggested that the Agencies exclude from the definition incidents that would result in violations of a banking organization's or a bank service provider's

policies and procedures, since these would be unlikely to rise to the level of a notification incident. Commenters also suggested that "computer-security incident" be refined to include only actual, rather than "potential" harm to a banking organization or service provider.

Some commenters stated that it was overly broad and unclear to define a notification incident by reference to a computer-security incident that "could" materially disrupt certain business lines or operations. Other commenters urged the Agencies to replace the "good faith" standard for notification incidents with a banking organization's or a bank service provider's "determination" that such an event had occurred. Commenters also suggested introducing materiality thresholds or excluding non-security related outages or incidents.

The Agencies also received comments requesting clarity on the methods of and means used for communicating the required notifications. Many commenters recommended flexibility in notification to the Agencies (including electronic communication and automated alerts). Some commenters also urged the Agencies to clarify the expected level of detail in the notification, and to adopt a joint notification process to streamline notification. Others urged the Agencies to clarify information-sharing practices relating to incident reports, expressing concerns with confidentiality and data security.

Several commenters expressed concerns with the timing of notifications. Some suggested that the Agencies revise the 36-hour timing for banking organization notifications with recommendations ranging from 48 hours to as long as 5 business days. Several commenters objected to the "immediate" notification requirement for bank service provider notifications to banking organization customers. Some recommended that the notification occur "as soon as practicable" after a service disruption. One commenter noted that an immediate notification standard may be appropriate, but only after the bank service provider has "determined" that a notification incident has occurred.

Commenters generally disagreed with the two-person notification requirement on bank service providers for banking organization customers. Commenters suggested that the Agencies allow the notification through existing processes or through general channels accessible by multiple employees at affected banking organizations. Some commenters asserted that requiring bank service providers to notify two contacts at each banking organization was overly prescriptive and burdensome. Instead, commenters recommended that bank service providers work with their banking organizations to designate a central point of contact, but also recommended that bank service providers not be required to ensure that a contact at the banking organization receive the notification.

Comments were also submitted on the practical impacts of the proposed rule. Several commenters contended that banking organizations would need to amend their contracts to comply with the rule. As an alternative to the proposed rule, some commenters urged the Agencies to accept the notification methods specified in these contracts and clarify contract expectations. But one commenter expressed concern that community banks might hold little power in these negotiations and recommended extending the compliance date of the rule for community banks.

Finally, some commenters believe that the proposed costs of compliance are significantly underestimated. These commenters suggest that the Agencies should gather more information and data to adequately assess the regulatory impact of the proposal.

THE FINAL RULE

The Agencies made a number of changes to the final rule in response to comments.

A. Revised Purpose Statement

The NPR's original purpose statement was to promote "the timely notification of significant computer-security incidents that affect FDIC-supervised institutions and their service providers." In response to comments received on the NPR, and to emphasize the materiality threshold of notification incidents, the Agencies qualified the purpose statement in the final rule to apply to "incidents that may materially and adversely affect FDIC-supervised institutions."

B. Revised Definition of Bank Service Provider to Exclude Designated Financial Market Utilities

In response to comments, the final rule excludes designated financial market utilities from the definition of bank service providers. The bank service provider definition now indicates, "no designated financial market utility shall be considered a bank service provider."

C. Added Definition of Covered Services

To clarify the scope of the final rule, the Agencies added a new definition for covered services, which includes "services performed, by a person, that are subject to the Bank Service Company Act (12 U.S.C. §§ 1861–1867)."

D. Revised Definition of Computer-Security Incident

The definition of "computer-security incident" was revised in the final rule and now states:

> *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.

The Agencies agreed with the observation that the existing NIST definition does not wholly align with the purposes of the proposed rule. The Agencies therefore removed the second prong of the proposed (NIST) definition relating to violations of internal policies or procedures. Further, a computer-security incident is now defined as an occurrence that has resulted in actual harm to an information system or the information contained within it. Staff believe these changes better suit the purposes of the rule, while retaining the general sense of, and consistency with, the NIST definition.

E. Added Definition of Designated Financial Market Utility

To clarify the exception to the bank service provider definition, the Agencies added a definition for designated financial market utilities, which "has the same meaning as set forth at 12 U.S.C. § 5462(4)."

F. Revised Definition of Notification Incident

In the final rule, "notification incident" was redefined as:

> [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.

First, to limit speculative or over-reporting, a notification incident is now defined as a computer-security incident that is "reasonably likely to" result in material disruptions, rather than incidents that "could" do so. Under this standard, a banking organization would be required to notify its primary federal regulator when it has suffered a computer-security incident that has a reasonable likelihood of inflicting material harm on the banking organization or its operations. Having thus narrowed the range of prospective harms that trigger a notification incident, the Agencies did not adopt the suggestion that "notification incident" be confined to reports of computer-security events that have already caused material harm to a bank.

Second, some commenters observed that the term "impair" contained in the proposed definition was redundant of "disrupt or degrade." They also noted that while NIST has defined "disrupt" and "degrade," NIST had not defined "impair." For these reasons, commenters suggested that "impair" be removed. The Agencies agreed, and have removed the term from the definition.

Finally, under the proposed rule a banking organization's notification obligation would have been triggered when it "believe[d] in good faith" that a computer-security incident materially threatened the operations of the organization. The Agencies agreed with commenters who criticized the original "believes in good faith" standard as subjective and imprecise. Accordingly, the Agencies revised the definition of "notification incident" to include incidents in which a banking organization "determines" that a computer-security incident has, or is reasonably likely to, cause harm to the institution in the material ways set forth by the remainder of the definition.

G. Notification to Agencies

The final rule leaves the agency notification language largely intact. The final rule states:

> A banking organization must notify the appropriate FDIC supervisory office, or 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.

The proposed 36-hour notification garnered a number of comments. Despite the expressed concerns, the Agencies have retained the 36-hour notification period for banking organizations to provide incident notification. The notification requirement is straightforward with no prescribed form or content. The definition of "computer-security incident" has been narrowed, and use of the term "determined" contemplates additional time to examine the nature of the incident—whether resulting from a security issue or a service disruption—to allow the banking organization time to assess the materiality of the disruption or degradation.

The final rule is designed to ensure that the responsible agency receives timely notice of significant emergent events, while providing flexibility to the banking organization to determine the content of the notification. A banking organization would be merely required to give notice to its primary federal regulator that it has determined a computer-security incident has affected, or in the bank's estimation is reasonably likely to materially affect the organization's operations or financial circumstances, or endanger the financial stability of the United States. Such a limited reporting requirement would alert the Agencies to such events without unduly burdening the banking organization with detailed reporting requirements.

H. Bank Service Provider Notification

After considering the comments, and following deliberations amongst Agency staff, the bank service provider notification requirement was revised in the final rule. That provision now states:

> (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.

Rather than requiring bank service providers to issue a notification to two individuals as in the proposed rule, the final rule requires bank service providers to notify "at least one bank-designated point of contact." If a bank has not designated a point of contact, the rule directs bank service providers to provide notice to "the [CEO] and [CIO] of the banking organization customer, or two individuals of comparable responsibilities, through any reasonable means." This would provide flexibility for the banking organization customers and the bank service providers alike. It would give the banking organization the ability to designate its preferred point of contact, while ensuring that, in the absence of such a designation, sufficiently senior bank personnel would be notified.

Multiple commenters suggested that the service provider notification requirement not apply to scheduled maintenance or other outages. The Agencies agree, and now expressly except such events from the rule.

The Agencies made a number of changes in this provision that will impact the timing of the bank service provider notification. First, the final rule has removed the "immediate" requirement, and replaced it with "as soon as possible." This change would encourage prompt notification, while removing what some commenters felt was an unrealistic standard. In addition, the final rule now

requires notification only after the bank service provider has "determined" it has experienced a computer-security incident. The use of the term "determined" here would give the bank service provider time to assess the materiality of the disruption or degradation of covered services. And, similar to changes made in the agency notification provision, the Agencies agreed to remove the term "impair" from this provision. Lastly, the "four or more hours" threshold should reduce notifications concerning less material incidents.

EFFECTIVE DATE AND EXTENDED COMPLIANCE DATE

The final rule would take effect on April 1, 2022; full compliance with the computer-security incident notification regulation would be extended to May 1, 2022.

RECOMMENDATION

Accordingly, staff recommends that the Board authorize for publication inthe *Federal Register* the attached final rule to amend 12 C.F.R. part 304.

STAFF CONTACTS

RMS Operational Risk:	Legal:	
Martin Henning (202) 898-3699	John Dorsey	(202) 898-3807
Rob Drozdowski (202) 898-3971	Graham Rehrig	(202) 898-3829