


April 12, 2021

Via Electronic Mail

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E–218
Washington, DC 20219

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

James P. Sheesley, Assistant Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Re: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Docket ID OCC–2020–0038 and RIN 1557–AF02; FRB Docket No. R–1736 and RIN 7100–AG06; FDIC RIN 3064–AF59)

Ladies and Gentlemen:

The American Bankers Association ("ABA"), Bank Policy Institute ("BPI"), Institute of International Bankers ("IIB"), and the Securities Industry and Financial Markets Association ("SIFMA") (collectively, the "Associations")[1] appreciate

[1] *See* Annex A for a description of each of the Associations.

the opportunity to comment on the notice of proposed rulemaking[2] issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the "Agencies") relating to computer-security incident notification requirements for banking organizations and their bank service providers. The Agencies' thoughtful review and study of cybersecurity issues is evident in the proposed rule, and the Associations welcome this positive step toward achieving clarity and consistency in the industry in this important area.

Like institutions throughout the public and private sectors, banking organizations are reliant on interrelated computer systems, and continue to be targeted in cybersecurity attacks. As such, our members recognize the importance of timely detection of significant cybersecurity threats, and fully support the Agencies' goal of ensuring timely awareness of these threats in order to promote the safety and soundness of the U.S. financial system.[3] In that regard, we appreciate the Agencies' recognition that a requirement that banking organizations timely notify the Agencies of critical cybersecurity incidents will represent the formalization of a voluntary practice that already exists.[4]

The Associations also strongly support the Agencies' efforts to minimize the regulatory burden placed on banking organizations addressing significant cybersecurity incidents, and to harmonize the proposed rule with existing definitions and notification standards.[5] Harmonization and other efforts to reduce additional burden will maximize banking organizations' ability to focus in a crisis on protecting their customers and restoring and ensuring the confidentiality, availability, and integrity of the systems on

---

2 Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 2299 (proposed Jan. 12, 2021) (to be codified at 12 C.F.R. pt. 53; 12 C.F.R. pt. 225, 12 C.F.R. pt. 304).

3 *See* 86 Fed. Reg. at 2301 ("The receipt of notification-incident information may give the agencies earlier awareness of emerging threats to individual banking organizations and, potentially, to the broader financial system[.]"); *id.* at 2302 ("The proposed rule would establish two primary requirements, which would promote the safety and soundness of banking organizations and be consistent with the agencies' authorities to supervise these entities.").

4 *See id.* at 2303 ("The agencies believe that in most cases banking organizations would eventually notify their primary regulator when an event occurs that meets the high threshold of a notification incident and that this proposed rule is formalizing a process that the agencies' experience suggest already exists.").

5 *See id.* at 2303 ("This proposal is not expected to add significant burden on banking organizations."); *id.* at 2304 (describing that the Agencies issued this proposed rule because existing "processes are not uniform or consistent between institutions and have not always resulted in timely notification being provided to the applicable regulator").

which their services and operations depend. We welcome the opportunity to collaborate with the Agencies on a rule that furthers our shared interest in this regard.

While the Associations support many aspects of the proposed rule, we believe change is warranted in several areas, and we propose revisions in those areas. Our recommendations are intended to bring additional clarity and consistency to the proposed incident notification framework, to ensure the Agencies receive timely notification of the significant cybersecurity incidents that are the focus of the proposed rule, and to minimize excess burden on banking organizations, including by avoiding unnecessary and burdensome over-reporting of less significant or easily remediated matters not intended to be captured by the proposed rule. We believe and intend that these proposed revisions will be workable for large and small institutions alike.

I. Executive Summary

- The Associations appreciate the Agencies' efforts to ensure clarity and consistency in the reporting of significant cyber incidents while minimizing the regulatory burden on banking organizations while responding to such incidents or otherwise in having to divert resources to unnecessary analysis and over-reporting of less significant or easily remediated events.

- While we support the policy goals of the proposed rule, we believe that, as currently drafted, the proposed rule calls for notification of incidents well below the intended threshold of critical cybersecurity incidents. As a result, the proposed rule would lead to significant and burdensome over-reporting to the Agencies, contrary to its stated intention. We provide recommendations that we believe will better achieve the shared goals of the Agencies and banking organizations in this context.

- In particular, the Associations suggest that the final rule reflect the following changes with respect to the notification requirements for banking organizations:[6]

    - The title of the rule should be changed from "Computer-Security Incident Notification" to reflect the rule's more limited scope and purpose.

    - The definition of "notification incident" should be revised.

        - The notification requirement should include only those incidents that result in "actual" harm and that a banking organization "determines" in good faith are "reasonably likely" to cause the significant harms set forth in the rule.

        - The notification requirement should be limited to information systems that carry out banking operations, activities, or processes,

---

[6] The Associations' suggested revisions to the text of the proposed rule are set forth in their entirety in Annex B.

or deliver banking products or services in the ordinary course of business, and should clarify that notification concerning material loss to a business line of revenue, profit or franchise value is only required if such loss is to the enterprise as a whole.

- The examples of notification incidents should be further clarified to provide guidance to banking organizations.

- The proposed 36-hour timeframe for notification will not be achievable or workable unless:

  - The definition of "notification incident" is tailored as set forth above;

  - The rule incorporates the shared view of the Agencies and banking organizations that it may require a reasonable amount of time for banking organizations to determine whether they have experienced a notification incident;

  - The timeframe is modified to require notification as soon as "practicable" but no later than 36 hours after the banking organization "determines" in good faith that a notification incident has occurred; and

  - The rule incorporates the shared view of the Agencies and banking organizations that notification need not include an assessment of the incident.

- The rule should permit banking organizations to provide notice through any of multiple potential channels.

- We welcome additional clarity on aspects of the post-notification process, including whether and to what extent the Agencies intend to share information provided in connection with a notification, how they intend to secure such information, and how they will ensure that examiners minimize excess burden on banking organizations dealing with potentially critical incidents.

- The definition of "banking organization" should be revised, including to add new financial services entities, such as non-bank OCC-chartered financial technology companies.

- We support the Agencies' efforts to hold bank service providers accountable to the banking organizations they serve, and to require them to provide prompt notification of disruptive incidents. In that regard, we recommend the following modifications to the bank service provider notification requirement:

- The proposed rule should be revised to allow for service providers to satisfy their notification requirement by providing notification to their banking organization customers consistent with any requirements and by any methods set forth by contract with that customer, so long as the method reasonably ensures that the banking organization receives the notification.

- The rule should require notification to be made where the bank service provider "determines" in good faith that a computer-security incident is "reasonably likely" to "materially" disrupt, degrade, or impair the relevant activities for four or more hours.

- The final rule should codify the Agencies' view, as articulated in the Preamble, that banking organizations would not be cited for the failure of a bank service provider to comply with the rule.

- Subsidiaries and affiliates should be excluded from the definition of "bank service provider" for purposes of the proposed rule.

- The rule should take effect no earlier than the first day of the calendar quarter beginning on or after 90 days following publication of the final rule.

II. Discussion of Comments on the Proposed Rule

A. Title of the Rule

We propose changing the title of the rule from "Computer-Security Incident Notification" to reflect the more limited set of incidents that would require notification under the rule, and we welcome the opportunity to work with the Agencies on devising a title. A change in nomenclature is important, in our view, in light of the rule's 36-hour timeframe for notification, which is significantly shorter than any existing cyber breach notification requirement in the industry. As set forth below, the rule's 36-hour timeframe will only be achievable, in our view, if the Agencies adopt the changes proposed herein. In the event that other regulatory bodies consider any notification timeframe as short as that in the proposed rule, we believe it is imperative that the rule be clear, including from its title, that it is limited to a narrow set of incidents, so that the adoption of this timeframe not be misperceived as achievable outside this limited context. "Computer-Security Incident Notification," by contrast, suggests a much broader set of incidents would be subject to notification under the rule than the rule actually requires.

B. The Definition of "Computer-Security Incident"

The proposed rule defines "computer-security incident" as "an occurrence that: (i) Results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information 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."[7] The Associations acknowledge and appreciate that the Agencies sought to align this term with an existing term from the National Institute of Standards and Technology ("NIST"). As a general matter, we believe that the existing NIST definition is overbroad for purposes of the rule. Consistent with the fact that the definition is not intended as a notification standard, the term "computer-security incident" captures a large volume of insignificant, everyday occurrences that will never rise to the level of a notification incident. We believe, however, that the term will be workable in the proposed rule so long as the definition of "notification incident" is more narrowly tailored, as we propose below, to achieve the rule's objectives.[8]

C. The Definition of "Notification Incident"

The proposed rule defines "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."[9] The Associations recognize and appreciate the Agencies' stated goal in drafting this definition to "minimize compliance burden by focusing only on events that are likely to cause significant harm to banking organizations," and to create only a "*de minimis*" regulatory burden, which is essential for any institution addressing a significant cybersecurity incident impacting its customers, services, operations or industry.[10] We also appreciate the Agencies' request for comment as to whether this definition should be modified.

While we support the policy goals of the proposed definition, we believe the definition should be tailored, consistent with the Agencies' intention, to avoid a

---

7 Proposed 12 C.F.R. pt. 53.2(b)(4), 86 Fed. Reg. at 2309; proposed 12 C.F.R. pt. 225.301(a), 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 304.22(b)(4), 86 Fed. Reg. at 2311.

8 The Associations emphasize, however, that if the NIST definition, which is the subject of ongoing discussion and analysis, is revised in the future, its definition within this rule should also be revised to maintain harmonization.

9 Proposed 12 C.F.R. pt. 53.2(b)(5), 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 225.301(a), 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 304.22(b)(5), 86 Fed. Reg. at 2311.

10 86 Fed. Reg. at 2305; *see also id.* ("The agencies believe that the regulatory burden associated with the notice requirement would be *de minimis* . . . .").

significant compliance burden on banking organizations in the form of over-reporting of less significant or easily remediated events. For the reasons set forth below, we propose revising the definition of "notification incident" as follows: "Notification incident is a computer-security incident that: (a) Results in actual harm to an information system that carries out banking operations, activities, or processes, or delivers banking products or services in the ordinary course of business; and (b) A banking organization determines in good faith is reasonably likely to 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, on an enterprise-wide basis, 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."

We believe this proposed definition will achieve the Agencies' goals while avoiding unnecessary burden and expense for banking organizations and the Agencies. In addition, we believe this definition will better harmonize the rule with banking organizations' existing, voluntary notification practices.

1. The notification requirement should be tailored to an incident that results in actual harm and that a banking organization determines in good faith is reasonably likely to cause the significant harms set forth in the rule.

First, we propose limiting the notification threshold to an occurrence that results in "actual" harm and that the banking organization "determines" in good faith is "reasonably likely" to cause the significant harms set forth in the rule. We believe this definition captures the full scope of incidents about which the Agencies seek early notification, while avoiding notification of innumerable, less significant incidents that are implied by the existing definition of "notification incident" in the proposed rule.

Specifically, as currently drafted, the proposed rule requires notification of any occurrence that results only in "potential" harm (since "computer-security incident" is defined in part as an occurrence that results in potential harm) and that the organization believes merely "could" cause the significant harms set forth in the rule. A notification requirement that includes "potential" harm, however, would capture occurrences of no consequence or utility in the proposed reporting framework that occur dozens or even hundreds of times a day at institutions across industries that would never result in the type of institution-wide or systemic impact contemplated by the proposed rule. For example, "potential" harm can be seen in garden-variety attempted bad acts by outsiders, including phishing emails and unsuccessful attempts to guess account passwords, among others; careless acts by an individual insider, including the loss of a securely password-protected laptop or mobile device, among others; insignificant software issues that institutions

address through automatic updates; and other frequent occurrences that result in no actual harm.

Further, defining "notification incident" to include any such incident that "could" materially disrupt, degrade, or impair certain significant activities, as set forth in the proposed rule, would inadvertently sweep up and require notification of countless less significant or easily remediated incidents because the majority of such incidents will pose at least a *theoretical* possibility of having a material impact—even if that possibility is highly remote and improbable. For example, a banking organization may promptly detect and remediate attempted unauthorized activity in certain accounts, or the compromise of an employee's email account in a phishing scheme, but the harms posed by such incidents "could" theoretically persist and be leveraged to cause greater harm despite a lack of any evidence and no reason to believe that they have done so.

To avoid over-reporting, the Associations propose tailoring the notification requirement to incidents that result in some "actual" harm that banking organizations "determine" in good faith are "reasonably likely" to result in the significant harms set forth in the rule. Incorporating this "reasonable likelihood" threshold will meet the goal of providing the Agencies with an early warning wherever a banking organization determines that such a harm may realistically occur. The Associations also propose replacing the word "believe" with the word "determine," which better captures the analytical process that must generally be undertaken by a banking organization before it can reasonably conclude that a notification incident has occurred, and which is used by the Agencies in the Preamble (*e.g.*, "[t]he proposed rule would require banking organizations to notify their primary federal regulator as soon as possible and no later than 36 hours after a banking organization has *determined* that a notification incident has occurred").[11]

2. The notification requirement should be more clearly defined with respect to the type of information systems and significant harms at issue.

The Associations believe that the notification requirement should also be more clearly defined with respect to the type of information systems and significant harms at issue. Specifically, the requirement should be limited to those information systems that may actually give rise to an incident of the type the Agencies are concerned about, that is, those that carry out banking operations, activities, or processes, or deliver banking products or services in the ordinary course of business. In our view, this delineation will achieve the Agencies' goal of ensuring timely notification of any "significant computer-security incident that could jeopardize the viability of the operations of an individual banking organization, result in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector"[12] because it includes the information systems of banking organizations that could give rise to such an incident. At the same time, we

---

[11] *Id.* at 2304 (emphasis added); *see also id.* at 2302–05, 2307–08.

[12] *Id.* at 2301.

believe the delineation avoids unnecessarily capturing myriad internal systems of banking organizations that have no effect on banking organizations' ability to provide products or services to customers, the banking organization's financial strength, or the stability of the financial system. For example, marketing systems and systems in which employee data is stored are information systems, but harm to these systems would not, by itself, result in any significant harm that is the focus of the proposed rule.

Separately, the proposed rule includes among notification incidents those that could materially disrupt, degrade or impair "[a]ny 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."[13] The Associations believe this category of reportable incidents should be narrowed to those that would, "on an enterprise-wide basis," result in a material loss of revenue, profit, or franchise value. Without this clarifying language, the rule may be construed to require notification to the Agencies of incidents that materially affect the value of any business line, including business lines that may be small and immaterial to the overall banking organization. The Associations believe that such a broad requirement would be inconsistent with the intention of the proposed rule.

3. The examples of notification incidents require further clarification to provide meaningful guidance to banking organizations.

Finally, while we appreciate that the Agencies have provided examples of incidents that would constitute notification incidents, we believe that some of the examples require additional detail to provide meaningful guidance, and otherwise would not necessarily meet the high threshold for notification that is intended by the Agencies. For example, while the first example, involving a distributed denial of service attack that disrupts access to customer accounts, is limited to attacks causing disruption "for an extended period of time (*e.g.*, more than 4 hours)," the third, sixth and seventh examples ("[a] failed system upgrade or change that results in widespread user outages for customers and bank employees," "[m]alware propagating on a banking organization's network that requires the banking organization to disengage all internet-based network connections," and "[a] ransom malware attack that encrypts a core banking system or backup data," respectively) do not currently include any limitation as to the length of time of disruption that would give rise to a notification incident.[14] From the customer's perspective, however, each of these incidents results in the same disruption of access to bank accounts or services. In addition, as to each of these examples, banking organizations may be able to remediate and resume operations promptly. For these reasons, we believe each example should

---

[13] Proposed 12 C.F.R. pt. 53.2(b)(5)(ii), 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 225.301(a), 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 304.22(b)(5)(ii), 86 Fed. Reg. at 2311.

[14] *See* 86 Fed. Reg. at 2302.

include, at a minimum, the same limitation that the disruption persists "for an extended period of time (*e.g.*, more than 4 hours)," and we would welcome further discussion about limiting the examples to those for which there is no near-term path to recovery for the institution. In addition, the example involving ransomware should be limited not only to attacks that result in encryption of core systems or data for an extended period of time, but as to which no backup system is available for an extended period of time.

In determining whether an incident rises to the level of a notification incident, banking organizations may consider other existing and potentially relevant regulatory and industry standards including capital and liquidity standards, or whether the occurrence constitutes a Sheltered Harbor event, among others. We welcome further discussion with the Agencies as to how banking organizations will assess the significance of the impact of potential notification incidents.

D. The 36-Hour Timeframe for Notification

The Associations appreciate the importance of early detection of significant cybersecurity incidents, and support the goal of ensuring early detection of emerging threats to individual banking organizations and the broader financial system. We also appreciate the Agencies' acknowledgment that, in requiring banking organizations to provide notification "as soon as possible and no later than 36 hours" after making a good faith determination that a notification incident has occurred,[15] the proposed rule would impose time-sensitive affirmative requirements on a banking organization, diverting crucial resources at the moment that the organization is responding to a significant security incident.[16] For a 36-hour notification timeframe to be potentially workable and achievable, it is imperative that the scope of the notification requirement be tailored as we have proposed above, and as further set forth below, to more closely align with the Agencies' limited intent in promulgating the rule.

1. The definition of "notification incident" should be revised as set forth herein.

As set forth above, we believe the term "notification incident" should be defined more precisely, as we have proposed above, to avoid unnecessary and burdensome over-reporting. Without these changes, the Associations do not believe the 36-hour timeframe is achievable or workable given the significant volume of incidents that would potentially constitute "notification incidents" under the proposed rule as drafted. With

---

15 *See* proposed 12 C.F.R. pt. 53.3, 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 225.303, 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 304.23, 86 Fed. Reg. at 2311.

16 *See* 86 Fed. Reg. at 2303 ("The agencies recognize that a banking organization may be working expeditiously to resolve the notification incident—either directly or through a bank service provider—at the time it would be expected to notify its primary federal regulator.").

these changes, however, and the others noted below, we believe the 36-hour timeframe would be both achievable and workable.

Additionally, in light of the new standard that the 36-hour notification timeframe represents for the industry, we think it is critical to tailor the definition of "notification incident" to the limited set of incidents that the Agencies intend to capture. To the extent any other regulatory bodies might consider a 36-hour timeframe for notification, it is critical that the language of this rule be precise as to its narrow application, because we believe this notification timeframe is not achievable or workable for banking organizations outside of this limited context.

2. The final rule should codify the Agencies' view, as set forth in the Preamble, that banking organizations may take a reasonable amount of time to determine whether a computer-security incident is a "notification incident."

We appreciate and support the Agencies' statement that they "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."[17] As the Agencies recognize, it typically requires review or investigation to determine the significance of any cybersecurity incident. For that reason, and to avoid over-reporting to the Agencies of incidents found to fall below the notification threshold after appropriate review or investigation is performed, we believe it is critical that banking organizations have comfort that they can conduct such review or investigation, consistent with the rule's notification requirements, before determining that a notification incident has occurred. In particular, the rule should incorporate the statement that after becoming aware of the potential occurrence of a notification incident, "the banking organization may take a reasonable amount of time to determine whether it has, in fact, experienced a notification incident."

Additionally, we appreciate the Agencies' use of the term "determine" in the Preamble with respect to a banking organization's conclusion that a notification incident has occurred (*i.e.*, the 36-hour time period begins running "after a banking organization has *determined* that a notification incident has occurred")[18] and we recommend that "determines" replace "believes" in the text of the rule, (*i.e.*, "determines in good faith," rather than "believes in good faith," that a notification incident has occurred).[19] In this regard, we note that it is not always clear when the "banking

---

17 *Id.* at 2302.

18 *Id.* at 2304.

19 Proposed 12 C.F.R. pt. 53.2(b)(5), 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 225.301(a), 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 304.22(b)(5), 86 Fed. Reg. at 2311.

organization," as opposed to any particular employee, has concluded that a significant cybersecurity incident has occurred. The nature and scope of cybersecurity incidents often do not manifest in immediately discernible or verifiable ways. Use of the word "determine" rather than "believe" would better capture the concept that appropriate review, investigation, internal discussion and/or analysis is typically required before a banking organization can conclude that any notification incident has occurred.

In this regard, we believe it is also important for the final rule to address an apparent misconception in the cost assessment of the proposed rule, which estimates that after a notification incident has occurred, and before notifying the Agencies, the incident may need to be escalated to and discussed with, and the response may need to be coordinated among, senior internal stakeholders such as the Chief Information Officer ("CIO"), Chief Information Security Officer ("CISO"), a senior legal or compliance officer, and staff of a bank service provider, as applicable, as well as senior management. Depending on the circumstances, and for banking organizations that rely on external parties to fulfill certain key stakeholder functions, it may be necessary for the banking organization to consult external counsel, cybersecurity firms, and other subject-matter experts. The proposed rule estimates that this process of notifying key stakeholders will take approximately three hours.[20] In banking organizations' experience, however, there are circumstances in which one employee, including any of the senior internal stakeholders identified by the Agencies, may conclude that a particular incident has occurred, while another (including any of the external subject-matter experts upon whom the banking organization may rely) may have questions or require follow-up work that indicates that such an incident has not occurred, is not significant, is easily remedied, or does not have particular legal or regulatory significance. In other words, it is not always the case that key stakeholders and advisers are merely apprised of the conclusion that a notification incident has occurred, such that their involvement entails merely three hours within a 36-hour timeframe for notification. Instead, the participation of these key stakeholders and advisers is in many cases crucial to the very determination of whether a notification incident has occurred such that the 36-hour timeframe can begin to run. We believe the Preamble and cost assessment should be revised to clarify this point.

3. The proposed rule should be modified to allow for notification as soon as "practicable" but no later than 36 hours after the banking organization determines in good faith that a notification incident has occurred.

We propose that the rule be modified to allow for notification as soon as "practicable," instead of as soon as "possible," but no later than 36 hours after the banking organization determines in good faith that a notification incident has occurred, and that the Agencies acknowledge in the Preamble that the time required to make a good faith determination that a notification incident has occurred may vary by banking organization and depending on the circumstances. The time required to make such a good faith

---

[20] 86 Fed. Reg. at 2304.

determination will naturally vary by banking organization, including between organizations that differ in size and available resources. The term "practicable," in our view, better captures that concept, avoiding any misperception that because one organization was able to conclude in a particular timeframe that a notification incident has occurred, it was "possible" that other organizations could have done so as well. By including this term, and the related acknowledgment in the Preamble, banking organizations will have comfort that as long as they report as soon as practicable for the organization and no later than 36 hours after determining that a notification incident has occurred, they will be in compliance with the rule even if another organization may have reached such a conclusion in a shorter timeframe.

4. The rule should incorporate the shared view of the agencies and banking organizations that notification need not include an assessment of the incident.

The Associations strongly support the Agencies' determination that "the notice would not need to include an assessment of the incident" or any specific information.[21] We believe that simplicity of the notification is critical to the effectiveness of the rule and, in particular, to the workability of a short 36-hour timeframe for notification. It is our view that requiring any specific information or assessment would result in a complex, uncertain, and burdensome process at a sensitive time. Given the significance of this issue for banking organizations, we believe it is important to incorporate this conclusion into the text of the rule itself.

E. The Notification Process

We appreciate the Agencies' solicitation of comments on the method of notification to the Agencies, and that the proposed rule already incorporates a degree of flexibility by allowing for notification through either written or oral communication. Rather than requiring notification solely to a single, agency-designated point of contact, however, we believe that providing banking organizations with multiple options for providing notification will best ensure that the Agencies receive timely notification, and in a manner that imposes a *de minimis* burden on institutions responding to a significant cybersecurity incident.[22]

1. The rule should provide banking organizations with multiple options for notifying the Agencies.

We agree with the Agencies' decision to allow notification through any technological means, but believe it is also critical to provide our members with multiple potential channels of communication of notification incidents. We recommend that the final rule provide that notification may be satisfied by any of several methods, including,

---

21 *Id.* at 2303.

22 *See id.* at 2305, 2307.

if applicable, notice to any member of the banking organization's on-site or supervisory team by any medium, notice to the regional office of the pertinent regulator, or notice to an agency-designated point of contact. We also recommend that the individuals to be contacted be mutually agreed upon by the parties.

During a disruptive incident, some channels of communication may not be operational or secure. Additionally, a banking organization may determine that it has experienced a notification incident during a holiday, at the start of a weekend, or at other times during which any particular method may be less desirable or any designated agency representative may be unavailable. Permitting notification to any of several points of contact and through multiple channels would help ensure that the Agencies receive the notification timely, and would reduce the burden on any banking organization in the event that a single designated point of contact were unavailable.

2. Post-notification communications and information-sharing should prioritize security and minimizing the burden on banking organizations.

Given the critical need for banking organizations to focus resources on response and recovery, and the Agencies' intention to impose only a *de minimis* burden in this context, we believe the Agencies should prioritize minimizing the burden on banking organizations in post-notification communications. For example, it will minimize the burden on banking organizations if they can set the cadence of post-notification communications after notification of an ongoing incident. Further, we believe that for the rule to operate as intended, it is critical that the Agencies communicate to examiners their stated intention, and the importance, of minimizing burden on banking organizations in this context, and that examiners adhere to that intention. We welcome the opportunity to discuss this issue further with the Agencies.

We also welcome further discussion about how the Agencies intend to share and secure any information provided by a banking organization in connection with a notification incident, an issue of critical importance to our members. For example, banking organizations would appreciate further clarity on how the Agencies envision securing the information once it has been received, and whether and under what circumstances the Agencies would share the information with other authorities. Given the sensitivity of the subject matter, we believe that notifications and any related information provided by a banking organization pursuant to the rule should be treated as confidential supervisory information that will not be made public.

F. The Definition of "Banking Organization"

We appreciate the Agencies' request for comments on the types of regulated entities that should be subject to the rule as "banking organizations." The definition of "banking organization" should include new financial services entities, including non-bank OCC-chartered financial technology companies. Notification incidents at such entities could result in systemic or disruptive effects similar to those at other types of banking

organizations, and information provided to the Agencies by these entities may assist the Agencies in supervising and advising other types of banking organizations.[23]

III. Bank Service Provider Notification

The proposed rule provides that a bank service provider "is required to notify at least two individuals at each affected banking organization customer immediately after the bank service provider experiences a computer security incident that it believes in good faith could disrupt, degrade, or impair services provided, subject to the Bank Service Company Act . . . for four or more hours."[24] The Associations appreciate the Agencies' recognition, in formulating this requirement, of the important role that bank service providers serve in the security of the banking system. We also support the Agencies' efforts to ensure bank service providers' accountability and notification to their banking organization customers about disruptive cybersecurity incidents, and their stated goal of minimizing the burden on banking organizations and bank service providers in this process. We also appreciate the statement in the Preamble that the Agencies would not cite a banking organization because a service provider fails to comply with the service provider notification requirement.[25]

Contrary to the Agencies' intention, we believe the proposed notification requirement would significantly increase the burden on banking organizations and their service providers. We propose revisions intended to provide further clarity on the nature and scope of the notification obligation in order to avoid this unintended consequence.

A. The Role of Contracts in the Notification Process

We understand from the Preamble that the Agencies would like to better understand the role that contracts play in ensuring that banking organizations receive notice of incidents from bank service providers. We appreciate that the Agencies have requested feedback on this issue, and agree with the Agencies that the existence of contractual

---

[23] The Associations also recommend that the Agencies exclude from the proposed definition of "banking organization" any systemically important financial market utility ("SIFMU") for which the SEC is the Supervisory Agency under Title VIII of the Dodd-Frank Act. The SEC's role as the primary rulemaking authority should be respected in connection with the development of technology incident management and notification standards. This is especially true in an area where, as in the case of Regulation SCI, the SEC has promulgated robust and effective regulatory requirements which would allow it to meet the objectives set forth in this Proposal.

[24] Proposed 12 C.F.R. pt. 53.4, 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 225.303, 86 Fed. Reg. at 2310; proposed 12 C.F.R. pt. 304.24, 86 Fed. Reg. at 2311.

[25] 86 Fed. Reg. at 2303.

obligations between banking organizations and service providers impacts the utility of the proposed rule.

The Agencies correctly state that "many existing contracts between banking organizations and bank service providers contain notification provisions regarding material incidents."[26] These contracts frequently establish the method of notification. The threshold and substance of what must be reported and the method of notification, as set forth in these contractual requirements, differs across banking organizations, and may differ within a banking organization. Factors that affect these differences include the nature of the service provider and its significance to the bank, how the relevant departments or divisions of the bank operate, the preexisting relationship between the bank and its service provider, and industry custom and practice with respect to the services at issue.

Many of our members are comfortable with the nature and scope of the contractual notification requirements imposed on their service providers, and the processes they have established for contractual notification to be provided. Importantly, many have drafted and negotiated these contracts in accordance with banks' obligations for third party risk management under existing interagency guidelines.[27] To comply with these guidelines, many banks have had to establish contractual expectations that address, among other things, breach notification requirements, including as to scope and timing, in a manner that is appropriate to the risk presented and taking into account the nature of the relationship. We believe that the rule should not supplant the contractual expectations these banks have carefully set forth in contracts, in part to meet their regulatory obligations. Doing so would impose a significant and unnecessary burden on these institutions, requiring them to renegotiate provisions that may number into the dozens or hundreds and that otherwise already meet the shared goals of the Agencies and banking organizations in this area. For example, many banking organizations contractually require service providers to provide notice of cybersecurity incidents using a different mechanism than the proposed rule's method of notifying two individuals of the banking organization. For instance, banking organizations may require service providers to report incidents through two *methods* (*e.g.*, an incident response hotline and email) rather than to two specific individuals.

For these reasons, we request that the proposed rule be revised to incorporate flexibility for the large group of institutions that manage these notifications by contract. Specifically, the proposed rule should be revised to allow for service providers to satisfy their notification requirement by providing notification to their banking customer

---

26 *Id.* at 2306.

27 *See, e.g.*, 12 C.F.R. pt. 30, appendix B; 12 CFR pt. 208, appendix D–2, 12 C.F.R. pt. 225, appendix F; 12 C.F.R. pt. 364, appendix B; *Outsourcing Technology Services*, FFIEC IT EXAMINATION HANDBOOK INFOBASE, https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/contract-issues.aspx (last visited Apr. 8, 2021).

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. Accordingly, we recommend that the final rule require bank service providers "to notify each affected banking organization customer, in a manner that reasonably ensures that the banking organization receives the notification, after the bank service provider experiences" a relevant incident.

B. Nature and Scope of Notification Requirement

We appreciate the Agencies' request for comments as to whether the bank service provider notification requirement should be limited in nature and scope in order to "only attach to a subset of services provided to banking organizations under the BSCA" or "to certain bank service providers, such as those that are examined by the federal banking Agencies."[28] We believe the proposed rule should be revised in this regard in order to avoid the risk that bank service providers substantially over-report. Over-reporting would create unnecessary burden not only for service providers, but for banking organizations, which may need to respond to such notifications by undertaking further assessment and analysis of the incident in order to assess the level of risk posed by the occurrence.

In addition, as with the proposed definition of "notification incident," the requirement that service providers report any computer-security incident that "*could* disrupt, degrade or impair services for four or more hours"[29] can be expected to lead to substantial over-reporting of less significant or easily remediated occurrences. The risk of such over-reporting is heightened by the proposed requirement that the service provider's notification be made "immediately." While banking organizations encourage immediate notification, we believe that the utility of that requirement depends upon the nature and quality of the notifications provided. We understand that bank service providers recommend that the rule require notification "timely," as opposed to "immediately," to enable them to assess the severity of a computer-security incident and minimize the risk of unnecessary notifications. We note, in addition, that certain banks and bank service providers have effective contractual provisions governing the timing of notification. We anticipate further discussion among banking organizations, bank service providers, and the Agencies to achieve a standard that achieves our shared goals and is workable for all parties.

Accordingly, the Associations believe the following revisions should be made to the service provider notification requirements:

---

[28] 86 Fed. Reg. at 2306.

[29] Proposed 12 C.F.R. pt. 53.4, 86 Fed. Reg. at 2310 (emphasis added); proposed 12 C.F.R. pt. 225.303, 86 Fed. Reg. at 2310 (emphasis added); proposed 12 C.F.R. pt 304.24, 86 Fed. Reg. at 2311 (emphasis added).

- *First*, bank service providers should be required to provide notice of reportable incidents that they determine in good faith are "reasonably likely" to "materially" disrupt, degrade, or impair the relevant services for four or more hours;

- *Second*, the notification requirement should be limited to critical services and bank service providers. We support the Agencies' suggestion that the rule may be limited to services or providers subject to specific supervisory programs to achieve the policy aims of the proposed rule without overburdening banking organizations and bank service providers with immaterial notifications. Programs that might be considered, but would require further discussion and analysis, include the Significant Service Provider ("SSP") Program for systemically important third-party service providers, and the Shared Application Software Review ("SASR") Program, which generally examines purchased software that involves mission-critical, core, or high-risk applications widely used at financial institutions.[30]

C. Enforcement

The Associations appreciate the Agencies' statement in the Preamble that banking organizations will not be cited for the failure of a bank service provider to comply with the rule.[31] Given the importance of this statement to our members, we request that the final rule incorporate the statement that "an affected banking organization is not responsible for the failure of a bank service provider to comply with this part." Relatedly, we understand that it will be unnecessary for banking organizations to modify their contracts to reference enforcement of the rule given the Agencies' intention to enforce the rule directly against bank service providers.

D. Definition of "Bank Service Provider"

Finally, we appreciate that the Agencies have requested comments on the proposed definition of "bank service provider." The Associations recommend that banking organization subsidiaries and affiliates be expressly exempt from the "bank service provider" definition. These entities already follow internal escalation processes to alert parent banking organizations to potential reportable incidents, and, as the Preamble to the proposed rule notes that these entities should continue doing so, their inclusion in the definition would be redundant. Their inclusion would also create an unnecessary potential burden on them to revise their existing, well-functioning processes to the extent those processes differ from those set forth in the rule. We would suggest that the revised

---

30 *Supervision of Technology Service Providers*, FFIEC IT EXAMINATION HANDBOOK INFOBASE, https://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers.aspx (last visited Apr. 8, 2021).

31 86 Fed. Reg. at 2303 ("Regulators would enforce the bank service provider notification requirement directly against bank service providers and would not cite a banking organization because a service provider fails to comply with the service provider notification requirement.").

definition provide as follows: "Bank service provider means a bank service company or other person providing services to a banking organization that is subject to the Bank Service Company Act (12 U.S.C. 1861–1867), *except that banking organization subsidiaries and affiliates are excluded from the definition of bank servicer provider for the purposes of this part*."

The Associations also recommend that the Agencies exclude from the proposed definition of "bank service provider" financial market utilities ("FMUs") as defined by the Dodd-Frank Act. Such entities have existing practices of providing timely notice to their primary federal regulator and bank customers of operational incidents. An FMU's direct notice to its primary federal regulator meets the Agencies' objectives set forth in the proposed rule in the most efficient and least burdensome way.

IV. Implementation

The Associations request that the proposed rule take effect no earlier than the first day of the calendar quarter beginning on or after 90 days following the publication date of the final rule. This timeframe would allow our members to take any necessary steps to prepare to comply with the rule. Further, when the final rule is promulgated, the Associations encourage the Agencies to communicate the promulgation of the final rule broadly to both banking organizations and bank service providers.

* * *

The Associations appreciate the opportunity to comment on the notice of proposed rulemaking. We intend to continue jointly discussing the proposed rule, and look forward to engaging in discussion with the Agencies in the post-comment period on the areas of the proposed rule that require further clarity.

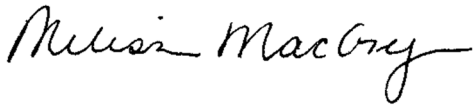
If you have any questions, please contact Paul Benda at (202) 663-5256 (*pbenda@aba.com*), Christopher Feeney at (202) 289-4322 (*chris.feeney@bpi.com*), Stephanie Webster at (646) 213-1149 (*swebster@iib.org*) or Melissa MacGregor at (202) 577-1997 (*mmacgregor@sifma.org*).

Respectfully submitted,

Paul Benda
Senior Vice President, Operational Risk and Cybersecurity
American Bankers Association

Christopher Feeney
EVP and President, BITS
Bank Policy Institute

Briget Polichene
Chief Executive Officer
Institute of International Bankers



Melissa MacGregor
Managing Director & Associate General Counsel
Securities Industry and Financial Markets Association

Annex A: The Associations

The American Bankers Association

The American Bankers Association is the voice of the nation's $21.9 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $17 trillion in deposits and extend nearly $11 trillion in loans. www.aba.com [aba.com]

The Bank Policy Institute

The Bank Policy Institute (BPI) is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth. For more information on BPI, visit http://www.bpi.com [bpi.com].

Institute of International Bankers

The Institute of International Bankers (IIB) is the only national association devoted exclusively to representing and advancing the interests of the international banking community in the United States. Its membership is comprised of internationally headquartered banking and financial institutions from over 35 countries around the world doing business in the United States. The IIB's mission is to help resolve the many special legislative, regulatory, tax and compliance issues confronting internationally headquartered institutions that engage in banking, securities and other financial activities in the United States. Through its advocacy efforts the IIB seeks results that are consistent with the U.S. policy of national treatment and appropriately limit the extraterritorial application of U.S. laws to the global operations of its member institutions. Further information is available at www.iib.org.

The Securities Industry and Financial Markets Association

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org [sifma.org].

Annex B: Text of Proposed Rule[1]

~~Computer-Security Incident Notification~~ [Placeholder for New Title]

§ [ ] Authority, purpose, and scope.

(a) *Authority*. This part is issued under the authority of [12 U.S.C.—].

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

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

§ [ ] Definitions.

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

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

(1) *Banking organization* means [relevant definition set forth in Agencies' proposals] **and new financial services entities, including non-bank OCC-chartered financial technology companies, except that systemically important financial market utilities for which the SEC is the Supervisory Agency under Title VIII of the Dodd-Frank Act are excluded from the definition of banking organization for the purposes of this part.**

(2) *Bank service provider* means a bank service company or other person providing services to a banking organization that is subject to the Bank Service Company Act (12 U.S.C. 1861– 1867)**, except that banking organization subsidiaries and affiliates and financial market utilities as defined by the Dodd-Frank Act are excluded from the definition of bank service provider for the purposes of this part.**

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

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

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

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

(5) *Notification incident* is a computer-security incident that:

(A) Results in actual harm to an information system that carries out banking operations, activities, or processes, or delivers banking products or services in the ordinary course of business; and

(B) a banking organization ~~believes~~ **determines** in good faith ~~could~~ **is reasonably likely to** 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**, on an enterprise-wide basis,** 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.

---

[1] Text in strike-through reflects proposed deletions, and text in bold reflects proposed additions, to the Agencies' proposed rule.

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

§ [ ] Notification.

A banking organization must notify the [relevant 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 [Agencies],~~ **notice to any member of the banking organization's on-site or supervisory team by any medium, notice to the regional office of the pertinent regulator, or notice to an agency-designated point of contact. The notice would not need to include an assessment of the incident.** The [relevant Agency] must receive this notification from the banking organization as soon as ~~possible~~ **practicable** and no later than 36 hours after the banking organization ~~believes~~ **determines** in good faith that a notification incident has occurred. **The banking organization may take a reasonable amount of time to determine whether it has, in fact, experienced a notification incident.**

§ [ ] Bank service provider notification.

A bank service provider is required to notify ~~at least two individuals at~~ each affected banking organization customer**, in a manner that reasonably ensures that the banking organization receives the notification,** immediately after the bank service provider experiences a computer-security incident that it believes in good faith ~~could~~ **is reasonably likely to materially** disrupt, degrade, or impair services provided, subject to the Bank Service Company Act (12 U.S.C. 1861–1867), for four or more hours. **An affected banking organization is not responsible for the failure of a bank service provider to comply with this part.**