Nancy L. Perkins
Nancy.Perkins@arnoldporter.com

+1 202.942.5065
+1 202.942.5999 Fax

601 Massachusetts Avenue, NW
Washington, DC 20001

April 12, 2021

Mr. James P. Sheesley
Assistant Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, D.C. 20429

Re: Comments on RIN 3064-AF59

Dear Mr. Sheesley:

Arnold & Porter Kaye Scholer LLP submits this letter on behalf of one of our major bank clients (the "Bank"), whose primary regulator is the Federal Deposit Insurance Corporation ("FDIC"), to provide comments on the proposal of the federal banking agencies ("Agencies") to adopt new Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (the "Proposed Rule").[1] The Bank has a strong interest in the Proposed Rule as a supplement to the current federal requirements for notification of data security incidents. As is true for any major banking organization, security incidents threaten to disrupt Bank operations and cause serious harm to the Bank and its clients. In general, the Bank supports adoption of the Proposed Rule, but with certain modifications, as detailed below.

I. Definitions

A. 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

[1] 86 Fed. Reg. 2299 (Jan. 12, 2021).

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

The Agencies have asked whether this definition should be narrowed to include only occurrences that result in *actual* harm or that constitute an *actual* violation of security policies or procedures. We do not believe that the definition should be so narrowed. If banking organizations were notified by their service providers only of *actual* computer-security incidents, harm will by definition already have occurred before a banking organization learns of an incident. To help prevent harm to an information system or information in that system, a banking organization needs to know there is a *threat* of harm (*i.e.*, the existence of "potential harm"). Similarly, if there is a threat of a violation of a security policy or procedure, the relevant bank needs to know that for the same reason: to help prevent harm that might result from such violation *before* it occurs.

Rather than narrowing the "computer-security incident, we believe the definition should be slightly broadened by replacing the word "imminent" in paragraph (ii) above with the word "serious." Again, if a bank is notified only when a policy or procedure violation is "imminent," the bank's ability to prevent harm is compromised. We do not believe it will unduly burden service providers to have to notify banks when they detect a serious threat of a policy or procedure violation.

B. "Notification Incident"

We do not believe there is a need for modification of the proposed definition of "notification incident." The Agencies have suggested that this definition could refer to terms used in the National Institute of Standards and Technology ("NIST") rather than to "computer-security incidents." We think it is appropriate to maintain the definitional link between incidents triggering notification *to* banking organizations and notifications required to be made *by* banking organizations.

We strongly urge the Agencies to maintain the qualifiers in the "notification incident" definition that limit its application to (i) "material" disruptions, degradations, or impairments, (ii) incidents affecting a bank's ability to service a "material" portion of its customer base, and (iii) incidents resulting in a "material" loss of revenue, profit or franchise value. We do not believe it would be beneficial or help serve the stated objectives of the proposed rule for the Agencies to receive notice of incidents that do not have a material impact in these specified ways.

C. Bank Service Provider

The Proposed Rule defines "bank service provider" as "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)." We believe the Agencies may have meant the phrase "that is subject to the Bank Service Company Act" to qualify "services" rather than "other person providing services" or "banking organization." This is our interpretation, despite the singular "**is**" subject, because (i) the persons providing services who are subject to the Bank Service Company Act *are* bank service companies, and (ii) banking organizations are "subject" to the Bank Service Company Act only insofar as they must seek prior approval before making an investment in a bank service company. We would therefore recommend that the word "is" be changed to "are" so that it is clear that what is referred to as "subject to the Bank Service Company Act" are the *services* that are permissible services for a bank service company under the Bank Service Company Act (which also may be performed for a banking organization by other persons).

II. Notification Procedures

A. Timeframes

The Agencies have asked whether the 36-hour timeframe for banking organizations to report "notification incidents" should be modified. We do not believe modification is needed, particularly because the Proposed Rule provides that this is an outer time limit -- that a banking organization should report to its primary regulator "as soon as possible." We do, however, believe that the final rule should expressly articulate the Agencies' explanation that the 36-hour timeframe commences at the point when a banking organization has determined in good faith that a notification incident has occurred.[2] We strongly recommend that the final rule incorporate this understanding in the text of the rule itself to provide clarity and certainty regarding the trigger for the start of the 36-hour timeframe.

In theory, we also support the requirement for service providers to notify banking organizations "immediately" after experiencing a computer security incident that meets the service provider notification standard (*i.e.*, when the service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair its services for a banking organization for four or more hours). We believe it is essential

---

[2] *See* 86 Fed. Reg. at 2,302.

that banking organizations be alerted to such incidents as soon as possible. We are concerned, however, that the "immediate" notification requirement could be considered by service providers as a standard with which compliance might be hard to demonstrate. We would suggest, for clarification and service provider reliance purposes, that the timeframe for services providers to provide notification to banking organizations be one (1) hour from the time at which the service provider determines that a computer-security incident it has experienced could disrupt, degrade or impair its services for such banking organizations.

B. Standard for Identifying Incidents as Reportable

The Agencies have asked whether the "good faith" belief trigger for notification by banking organizations and by service providers is an appropriate standard or whether, for example, "reasonably believes" would be preferable for notification by either or both types of entities. We believe the "good faith" belief standard is preferable to "reasonably believes" but that, in the case of service provider notifications, the trigger should be phrased in the negative, so that notification will be required ***unless*** the service provider has a good faith belief that the computer-security incident at issue does ***not*** pose the risk that would merit notification. Specifically, we recommend that the proposed standard for notification by service providers be revised as follows:

> A bank service provider is required to notify at least two individuals at each affected banking organization customer ~~immediately~~ within one hour after the bank service provider experiences a computer-security incident~~, that it~~ unless the service provider believes in good faith that the incident could not disrupt, degrade, or impair services provided subject to the Bank Service Company Act (12 U.S.C. 1861–1867) for four or more hours.

With respect to banking organization notifications to the FDIC, we also believe the "good faith" standard is appropriate but that it should be contextualized slightly differently, to help clarify the start of the 36-hour timeframe for notification. Specifically, we recommend that the proposed standard for notification by banking organizations be revised as follows:

> A banking organization must notify the FDIC of a notification incident through any form of written or oral communication, including through any technological means, to a designated point of contact identified by the FDIC. The ~~FDIC must receive this notification from the~~

> banking organization must provide this notification as soon as possible and no later than 36 hours after the banking organization has reached a good-faith determination ~~believes in good faith~~ that a notification incident has occurred.

C. Recipients of Bank Service Provider Notifications

The Agencies have asked if the final rule should require a bank service provider that experiences a notification-qualifying computer-security incident to notify *all* of the service provider's banking organization customers, or rather (as the Proposed Rule requires) just the banking organization customer(s) affected by the computer-security incident. We believe broader notification is warranted, for two related reasons. First, a computer-security incident may have a broader impact than is initially apparent, and early notice to all banking organization customers will allow each of them independently to consider and investigate any possible adverse impact on their operations, which may prevent harm. Second, even if a computer-security incident will not affect one or more banking organization customers, notice of the incident to all of them can put those banking organizations on alert to take additional precautions to prevent harm from any similar future incident (such as many banking organizations did upon learning of the SolarWinds data security breach).

The Agencies have also asked whether it would be unduly burdensome to require certain bank service providers, such as smaller bank service providers, to provide notice of material disruptions, degradations, or impairments that could constitute a notification incident for their affected banking organization customers, but where the customers would not be aware of the incident. We believe such a requirement would not be overly burdensome, even for smaller bank service providers, so long as the required mode of notification is not cumbersome, inconvenient, or expensive (such as the methods suggested in section II.D below ("Form of Notification"). And we believe it is critical for bank service providers to be required to provide notice in such cases; for example, if the service provider is hosting a subsystem of bank computerized data and the subsystem undergoes a material disruption, the banking organization would be unaware of the disruption until attempting to access the subsystem. Absent required notification, between the time the bank service provider discovers the incident and the time the banking organization tries to access the subsystem, there could be material harm to the banking organization's clients and/or the banking organization's relationships with its clients.

D. Form of Notification

The Agencies have expressed interest in what mode of communication is typically required for bank service provider notification of security incidents under service provider-banking organization contracts. The Bank generally requires two-fold notification: a phone call to the Bank's public contact number, which is channeled to relevant bank officials (including the Chief Information Security Officer), as well as an email to an email address shared by multiple Bank officials (as periodically designated by the Bank), which relieves the service provider of maintaining email addresses of the relevant officials, who may change over time.

III. Scope of Application

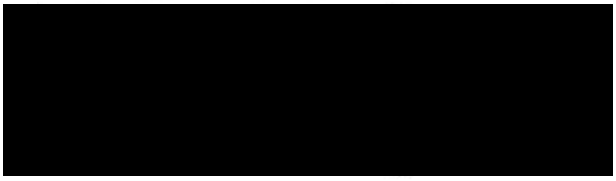
The Agencies have asked whether additional types of entities should be added to the definition of "banking organizations" that would be subject to the new rule. We believe this should be done -- that achieving the Agencies' goals for the rule will require including additional types of entities within the scope of the rule. Currently, the definition only encompasses FDIC-supervised insured depository institutions, but the banking system is rapidly expanding to include other types of institutions that likely will merit oversight by the FDIC. Accordingly, we recommend that the "banking organization" definition in the proposed rule be revised as follows:

> *Banking organization* means any FDIC-supervised <u>organization other than a bank service provider, including but not limited to</u> insured depository institution<u>s</u>, including all insured state nonmember banks, insured state-licensed branches of foreign banks, and State savings associations.

* * *

We appreciate your consideration of these comments. If you have any questions or need further information, please contact either me by e-mail (Nancy.Perkins@arnoldporter.com) or phone (202.942.5065).

Respectfully submitted,



Nancy L. Perkins