April 12, 2021

Brian P. Brooks
Acting Comptroller of the Currency
400 7th Street SW
Suite 3E-218, mail stop 9W-11
Washington, DC 20219

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

James P. Sheesley
Assistant Executive Secretary
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

BSA | The Software Alliance ("BSA") is grateful for the opportunity to provide preliminary feedback on the Notice of Proposed Rulemaking ("NPRM") regarding potential Computer-Security Incident Notification Requirements for Banking Organizations and Their Banking Service Providers.[1] BSA is the leading advocate for the global software industry. Our members provide services across the financial services industry and thus have deep insight into the challenges of securing the industry against the threats that it faces.[2] As global

---

[1] *See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 2299 (Jan. 12, 2021) (hereinafter "NPRM").

[2] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

corporations, we also have a shared interest in protecting the integrity of the U.S. financial system. BSA therefore applauds the underlying objectives of the NPRM.

We recognize the important supervisory interest the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Federal Reserve (collectively, the "Agencies") have in receiving timely notifications about "significant computer-security incident(s) 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." We likewise recognize that banking service providers play a critical role in enabling their banking customers to meet their regulatory obligations. A properly scoped computer-security incident notification requirement can facilitate the timely sharing of actionable information about ongoing threats between stakeholders and regulators in a manner that enhances collective security interests. Rather than establishing a new compliance "burden," an effective incident notification framework can foster partnership between impacted stakeholders and encourage greater proactive cooperation. To accomplish these objectives, the cyber-incident notification requirement should assign roles and responsibilities that are both clearly defined and targeted to ensure that the information being shared is actionable. While the NPRM largely hits the mark, we highlight two aspects of the proposed rule that would benefit from clarification.

1. The Definition of "Computer-Security Incident" is Ambiguous and Overbroad

Pursuant to the proposed rule, banking service providers will be required to provide notification to their banking customers upon experiencing a "computer-security incident that it believes in good faith could disrupt, degrade, or impair services…for four or more hours." The term "computer-security incident" is defined as an "occurrence" that either "(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."

We recommend a narrowing of the "computer-security incident" definition so that it focuses only on circumstances where there is evidence of actual harm. The reference to "potential harm" – particularly in combination with the requirement to provide notification for incidents that "***could***" result in service disruption – renders the rule highly ambiguous. A requirement to provide notification in circumstances where there is no evidence of an actual harm or service disruption is also far too broad. One of the key security benefits of modern cloud service providers is their ability to identify and block anomalous cyber activity using automated processes. Depending on the nature of the service, a cloud provider may detect and analyze over 8 trillion threat signals on behalf of their customers every day.[3] Requiring service providers to notify all of their customers each time they identify a threat with the potential to cause harm would quickly exhaust resources, not only of the service providers, but of their

[3] *See, e.g.,* New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security (August 2020) available at https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/.

banking customers that will have to receive, analyze, and address the notifications from all their applicable service providers.

In addition to removing the "potential harm" reference in the first prong of the definition, we recommend the elimination of the second prong of the definition in its entirety. Tying the notification obligation to the "violation or imminent threat of violation of security policies, security procedures, or acceptable use policies" implicates the same concerns noted above. A requirement that is triggered by the potential violation of a service provider's internal policies, even when there is no evidence of actual harm, will necessitate the sending of notices about events that are far removed from the type of cyber incident that this NPRM is intended to address. Because the definition extends to "acceptable use policies" that may be entirely unrelated to security, service providers may feel compelled to notify their financial services customers about events that do not warrant a security response from the financial institution, increasing effort from the customer's response team and directing security and reporting resources away from more critical activities.

- ***Recommendation:***

> *(1) 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.~~*

2. <u>The "Immediate" Notification Requirement for Banking Service Providers May Undermine the Objectives of the Proposed Rule</u>

The NPRM requires a service provider to notify its banking customers "immediately" after experiencing a computer-security incident that the service provider "believes in good faith could disrupt, degrade, or impair services…for four or more hours." The NPRM suggests that an "immediate" notification requirement is reasonable "because the notice would not need to include an assessment of the incident." Be that as it may, the purpose of the rule is to ensure that banking organizations receive notification when their service provider has a "good faith" belief that a cyber-security incident may "disrupt, degrade, or impair" services for more than four hours. It is unclear how the immediate notification requirement – which is pegged to the occurrence of the underlying computer-security incident – would allow for the service provider to undertake the type of investigation that would be necessary to make "good faith" determination about the severity of the event and the likelihood it may give rise to a service disruption.

Moreover, an immediate notification requirement is ultimately inconsistent with the goals of the NPRM, which seeks to "enable a banking organization to promptly respond to an incident, determine whether it must notify its primary federal regulator that a notification incident has occurred, and take other appropriate measures related to the incident." Rather than helping banking organizations identify material threats and develop informed responses, an immediate notification requirement would result in banks being inundated with a high volume of notifications that would be devoid of any meaningful content, actionable intelligence, or necessary context. In this regard, the immediate notification requirement could have the

unintended effect of undermining a bank's security efforts by forcing it to devote resources to analyzing and triaging low-information notices relating to cyber incidents that ultimately have no impact on the stability or availability of the third-party services on which they rely.

- ***Recommendation:***

  § 53.4 Bank service provider notification.

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

* * * * * * *

We appreciate the opportunity to share our members' perspectives on these important issues. BSA and its members are strongly committed to promoting the resilience of the financial sector and share the interest of the Office of the Comptroller of the Currency, the Federal Reserve Board, and the FDIC in promoting effective information sharing. We welcome the opportunity to continue the dialogue on this important topic.

Sincerely,

Christian Troncoso
Senior Director, Policy