April 12, 2021

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

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

The Honorable James P. Sheesly
Assistant Executive Secretary
Attn: 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*** (***OCC:*** *Docket ID OCC-2020-0038, RIN 1557-AF02;* ***Federal Reserve System:*** *Docket No. R-1736, RIN 7100-AF;* ***FDIC:*** *RIN 3064-AF59)*

Dear Madam or Sir:

Internet Association[1] (IA) appreciates the opportunity to provide comments on the joint notice of proposed rulemaking issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve Board System, and Federal Deposit Insurance Corporation (Agencies) regarding the notification requirements associated with a computer-security, or cyber, incident that has impacted a banking organization or a bank service provider.[2]

IA applauds the Agencies for working to develop an incident response strategy. Being able to respond to outages caused by both malicious actors as well as innocent but unexpected events in a manner that maintains the trust and confidence of the financial sector's integrity is paramount. With 95% of financial services firms (39% of whom were in the banking sector, specifically) indicating that they are discussing "cybersecurity and tech risks four times more per year" than they used to, the financial sector has taken the right steps towards maintaining a secure ICT infrastructure.[3] As such, the Agencies would be hard

[1] Internet Association represents the world's leading internet companies and supports policies that promote and enable innovation, increased consumer access to the financial system, and the responsible use of technology by banking organizations and the regulators who supervise them. Many of our members have cloud-based services that are used by banking organizations and their employees in order to improve their organization's operational resiliency, their internal efficiency, their user experience, as well as a number of other enterprise-wide activities.
[2] *See* Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 FR 2299 (proposed January 12, 2021).
[3] *See* Bank Policy Institute, "Cybersecurity: Emerging Challenges and Solutions for the Boards of Financial Services Companies", Exhibits 1 and 2,

pressed to find a responsible banking institution that does not have some form of contractual-based notification requirement in place already.

While the Agencies have recognized the importance of information sharing and timely coordination of a response to cyber incidents, there is room for deep and substantive collaboration with others: the Cybersecurity & Infrastructure Security Agency (CISA) with their ability to monitor and respond to cyber incidents and their participation in information sharing communities, like the Financial Services Information Sharing Community (FS-ISAC); General Services Administration (GSA) with their security certifications available through the FedRAMP Program Management Office (PMO); and industry itself with an ability to draw on experiences working with these agencies and related organizations worldwide.

This is especially true as it relates to the definitions of a relevant incident, requirements surrounding notification timelines, accounting for the shared responsibility model when it comes to cloud-based infrastructure, as well as when and how notification should be made.

With the above in mind and addressing specifically those issues within these Request for Comments that impact a bank service provider offering information and communication technology (ICT) products and services, we respectfully provide the Agencies with the following feedback:

1. Narrow the Definition of Computer-Security Incident to Cover Confirmed Events
2. Adopt a Flexible Mechanism for Bank Service Providers to Notify Their Bank Customers
3. Acknowledge the Shared Responsibility Model in Notification Requirements
4. Adopt an Alternative Approach to Making a Good Faith Estimate
5. Adopt a Joint Notification Process and Ensure Confidentiality

1. Narrow the Definition of Computer-Security Incident to Cover Confirmed Events

IA recommends a narrower definition of "computer-security incident" to ensure it covers actual harm to a customer's content and an actual breach of the bank service provider's network. While IA applauds the Agencies following the recommendations of the National Institute of Standards and Technology (NIST) in defining "an organization-specific definition" for what would constitute a "computer-security incident" that would be applicable to the proposed rule, the definition is too broad, leaving the scope unclear.[4]

Specifically, the speculative components in the proposed definition, including "potential harm" in (i) and "imminent threat" in (ii) will undoubtedly lead to several unintended consequences that will damage the effectiveness of the proposed rule and associated policy.

First, bank customers of service providers, and consequently federal regulators, could be flooded with meaningless notifications since there are many potential or suspected breaches that do not materialize into confirmed breaches.[5] Second, firms may interpret "potential harms" and "imminent threats"

---

https://bpi.com/cybersecurity-emerging-challenges-and-solutions-for-the-boards-of-financial-services-companies/ (September 29, 2020)

[4] *See* National Institute of Standards and Technology, Computer Security Incident Handling Guide, SP 800-61r2, https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final, page 6 (August 6, 2012)

[5] It is noted that a similar situation occurred to the Consumer Protection Safety Commission (CPSC) where a broader than useful definition of potentially recall-related retail information has led to an absolute deluge of data, leaving the team unable to review all submitted information, leading to

inconsistently. Third, notification of suspected breaches could add fear, uncertainty and doubt (FUD) instead of empowering the organization that receives the notice with reliable and meaningful information so that the organization can take appropriate action.

Narrowing the definition while also providing a non-exhaustive list of "notification incidents" that will remove ambiguity concerning what is and isn't reportable will give the teams within the Agencies, banks, and bank service providers a mandate to focus only on those incidents that are actually causing harm will ensure these incidents are mitigated appropriately, while those future and potential issues are managed by the teams within each organization that has the appropriate levels of access and accountability to escalate when appropriate.

2. Adopt a Flexible Mechanism for Bank Service Providers to Notify Their Bank Customers

IA recommends a focused and flexible approach to notification requirements to ensure it provides banks and bank service providers the ability to utilize the notification procedures that work best for them. While IA understands the intent of the Agencies to require a particular process for notification that will improve the chances an incident is responded to appropriately, ensuring alternate methods that still achieve the same outcomes are acceptable will keep banking ICT systems safe as internal workflows evolve.

Specifically, the prescriptive requirements, such as requiring "two individuals" be notified", rather than focusing on the outcomes, such as ensuring the appropriate individuals or entities at a bank are notified, will ensure incidents are addressed in a timely fashion.

First, the Agencies would potentially override existing contractual clauses and obligations. Second, firms may actually result in losing time to respond if the "two individuals" or other prescriptive requirements are slower than existing processes. Third, future methods of notification could be stymied as a result of meeting compliance requirements rather than mitigation ones.

Focusing on "prompt" notification, not to exceed 72 hours, rather than "immediate" notification will ensure banks and their service providers have the time necessary to perform joint due diligence and to develop a solution that will mitigate the impact to their own impacted systems while also help any other potentially impacted organizations to identify if they are vulnerable, protect themselves, detect any harm that may have been caused, and then to respond and recover appropriately.[6]

3. Acknowledge the Shared Responsibility Model in Notification Requirements

IA recommends that the Agencies more explicitly account for the differences in responding to an incident based on the service delivery method in order to ensure organizations account for the shared responsibility model. While IA applauds the fact the Agencies do not expect bank service providers to "assess whether [an] incident rises to the level of notification", the work required to address an

---

Congress proposing the use of artificial intelligence (AI) and machine learning (ML) to save the staff from buckling. Failing to look at just those incidents that require a response is not only unsustainable, it is a failure to follow an established best practice.

[6] These five functions - Identify, Protect, Detect, Respond, and Recover - are a part of the internationally recognized NIST Cybersecurity Framework, created through private- and public-sector collaboration to create a "prioritized, flexible, repeatable, and cost-effective approach" to deal with cybersecurity issues. *See* Cybersecurity Framework Version 1.1, https://www.nist.gov/cyberframework (April 16, 2018)

on-premises incident versus a cloud-based one differ significantly.

Specifically, when determining whether an incident rises to the level of requiring notification, the type of technology used to deliver the service should be accounted for in determining whether the responsibility to address the incident lies with the bank, the bank service provider, or both.

First, responding to incidents involving on-premises ICT systems versus cloud-based ones will differ due to the way in which the shared responsibility model shifts some responsibilities to the cloud service provider (CSP) while an on-premises solution leaves most in the hands of the bank. Second, acknowledging the roles of each in securing and maintaining access to sensitive data must be accounted for when determining whether a notification is required to be made by the bank service provider or the bank itself. Third, clarifying the differences between the two service delivery models will also provide Agencies with the ability to better react when notified.

Developing notification requirements based on the manner in which a bank uses a bank service provider will ensure the roles and responsibilities of all those involved in responding to an incident are not confused when it matters most. A bank service provider should not be forced into the middle of a situation into which it may have no visibility, especially if an incident is within the domain of the bank's portion of the shared responsibility model.

4. Adopt an Alternative Approach to Making a Good Faith Estimate

IA recommends the Agencies account for the shared responsibility model when determining whether a bank service provider has the ability to notify a bank of an issue that could impact their ICT systems. While IA applauds the specificity with which an event must be analyzed to determine if it requires notification, the existing "good faith" standard is problematic for any cloud-based bank services.

Specifically, due to the way in which CSPs are unable to actually access and review the data of a bank in the same way an on-premises solution provider would, such a requirement would be impossible to comply with in some instances and very difficult in most others.

First, because CSPs are unable to access the type of customer data that would be necessary to determine the downstream impact of certain incidents, developing a "good faith" belief would be subjective and inconsistent as it would be speculative. Second, in order to err on the side of caution, failing to address this issue would result in additional false positives as a defense mechanism against a rule that is incompatible with the manner in which cloud-based technology is implemented. Third, such a deluge of false positives would harm the ability of Agencies to be able to prioritize incidents based on their actual risk to the financial system.

Modifying the standard to require "prompt" notification upon a bank service provider obtaining actual knowledge of "an incident that could disrupt, degrade, or impair services for four or more hours" would ensure only real issues are escalated and that all service delivery methods would be accounted for in the notification requirements.

5. Adopt a Joint Notification Process and Ensure Confidentiality

IA recommends the Agencies provide for joint notification requirements that are built on a foundation of confidential information sharing between banks, bank service providers, and the Agencies themselves.

While IA members appreciate the unique challenges each banking organization and their associated regulator will face when responding to a cyber incident, a constant truth that will transcend all service delivery models and organizational concerns is that time is of the essence.

Specifically, making sure banking organizations that are large enough to be subject to different notifications from different entities are able to notify one agency, keeping their focus on mitigating and eliminating the threat.

First, requiring multiple notifications to a number of agencies with differing notification requirements costs precious time and resources that should be spent on the intended outcome of this rule - stopping and recovering from cyber incidents. Second, failing to provide the appropriate safeguards to allow organizations to be confident that the incredibly sensitive information they share will be safeguarded will harm the ability of security professionals to respond properly, not just at those who were impacted. Third, failure to coordinate among the agencies who have a mandate to address the supervisory and regulatory concerns that will arise out of any cyber incident will severely diminish the ability of the Agencies to take a holistic approach to cybersecurity.

Streamlining the notification process to incentivize safe and secure communications and collaboration among industry and government will be essential to securing not just the financial sector, but the ICT supply chain it relies on to improve and increase access to financial services.

In conclusion, the Agencies must ensure any cybersecurity requirements, including notification requirements, are developed with both legacy ICT services and modern infrastructure in mind, especially as the financial services industry continues to digitize and adopt cloud-native features and functionality.

IA appreciates the opportunity to comment on this proposed rule and looks forward to working with the Agencies as they work to promote safe and secure innovation in America's financial system. Please do not hesitate to reach out with questions or to discuss our comments in further detail.