Mindset

April 12, 2021

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street, SW, Suite 3E–218 Washington, DC 20219
Docket ID OCC–2020–0038
RIN 1557-AF02

James P. Sheesley
Assistant Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
RIN 3064-AF59

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Docket No. R-1736 RIN 7100-AG06

RE: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, Docket ID OCC-2020-0038

Dear Sirs or Madams:

I write on behalf of the Insurance Coalition ("the Coalition"), a group of federally supervised insurance companies that share a common interest in federal regulations affecting insurers. Regarding cybersecurity, insurance companies rely on the trust of their policyholders as a core part of their business model. As heavily regulated firms, adhering to the highest standards of cybersecurity preparedness is not only a regulatory requirement; it is necessary to maintain long-term relationships with policyholders and their families, sometimes spanning generations. In addition, members of the Coalition work closely with their state insurance regulators to ensure the dynamic challenges posed by increasingly sophisticated hackers are addressed collaboratively.

As such, we support your efforts to provide for timely notice of a significant cyber event to appropriate regulatory entities. With nation-states and other well-funded groups intensifying their focus on the financial sector, it is important that regulators are provided critical information that can be used to the benefit of the entire ecosystem and the customers our

members serve. To best accomplish this, we believe any new notice requirements should strive to create clarity and consistency, and be focused on responding with actionable information on the most serious of cyber-related incidents. To that end, we have provided the following responses to certain questions from your proposal entitled “Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers” (“the Proposal”). In general, we align ourselves with comments submitted by other industry stakeholders, such as the American Bankers Association.

Responses to Relevant Questions

Question 1: How should the definition of “computer-security incident” be modified, if at all? For example, should it include only occurrences that result in actual harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits? Should it include only occurrences that constitute an actual violation of security policies, security procedures, or acceptable use policies?

The Proposal defines a “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 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.”

Of the two key terms defined in the proposal – “notification incident” being the other – a “computer-security incident” is a lower threshold of severity and as such does not require notice to regulators when one occurs. However, we agree that it is prudent to include the *potential* for harm in this definition. Doing so would better align with what is likely to be the ongoing process within a banking organization to assess the nature and scope of the incident itself.

However, the language is cause for confusion: As currently drafted a firm would need to evaluate whether an incident “results…in potential harm….” Effectively, this asks firms to prove that the potential harm of an event has actually resulted in said harm, which could make determining when an event qualifies as a “computer-security incident” challenging.

We believe a clearer approach to a definition of “computer-security incident” would be: An event that *has or may result in harm* to the confidentiality, integrity, or availability of an information system….” This same construction could be used in the context of actual or potential violations of security policies as well.

Question 2: How should the definition of “notification incident” be modified, if at all? For example, instead of “computer-security incident,” should the definition of “notification incident” refer to other NIST terms and definitions, or another recognized source of terms and definitions? Should the standard for materially disrupt, degrade, or impair be altered to reduce potential redundancy between the terms or to consider different types of impact on the banking organization? Should the definition not include language that is consistent with the “core business line” and “critical

operation" definitions included in the resolution-planning rule? Should those elements of the definition only apply to banking organizations that have resolution planning requirements?

How should the definition of "notification incident" be modified, if at all?

The Proposal defines a "notification incident as "…a 'computer-security incident' that a banking organization believes in good faith could materially disrupt, degrade, or impair –

- The ability of the bank 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;
- Any business line of a bank, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or
- Those operations of a bank, 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."

Here, and as we will describe in response to subsequent questions, we believe this definition should be improved by more clearly linking the point at which a "computer-security incident" becomes a "notification incident" to the risk determination a banking organization needs to make as it assesses the impact of a cyber incident.

Investigations of cyber incidents are often dynamic, forensic processes that evolve moment-to-moment. While the language in the Proposal refers to a "good faith" belief, providing a clearer moment-in-time delineation between the two key types of cyber incidents, and incorporating clearer risk of harm thresholds (similar to what we proposed in Question 1), would facilitate the process of a banking organization making a determination that a "computer-security incident" is serious enough to rise to the level of a "notification incident."

For example, we believe the appropriate approach should be:

A "computer-security incident" becomes a "notification incident" when a banking organization *determines there is a reasonable risk* that the "computer-security incident" *has resulted in or will result in* material disruption or degradation of…."

This construction incorporates time, risk, and the scale of the problem, all of which are assessments critical for the banking organization and regulators.

Should the standard for materially disrupt, degrade, or impair be altered to reduce potential redundancy between the terms or to consider different types of impact on the banking organization?

We believe this portion of the definition of "notification incident" includes overlapping and redundant terms and should be modified. For example, if a computer system is "disrupted" or "degraded," it is certainly also "impaired." However, a process could be "degraded" without being "disrupted." Thus, we recommend dropping the concept of "impairment," as the previous section of our response to this question reflects.

Question 3: How should the 36 hour timeframe for notification be modified, if at all, and why? Should it be made shorter or longer? Should it start at a different time? Should the timeframe be modified for certain types of notification incidents or banking organizations (for example, should banks with total assets of less than $10 billion have a different timeframe)?

As currently drafted, the Proposal requires a banking organization to notify its primary federal regulator "as soon as possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred." As a threshold matter, we believe a 36-hour window for notification may be appropriate, but only if the definition of "notification incident" is modified as we have proposed above, or in a similar way. In addition, as we have previously discussed, for clarity and consistency, we believe the start of the 36-hour window should be linked to the *determination* a banking organization would need to make that a "computer-security incident" has risen to the level of a "notification incident."

Therefore, we recommend the Proposal be modified to state that notification to a primary federal regulator shall occur "as soon as practicable and no later than 36 hours after the banking organization determines that a computer-security incident is a notification incident."

We do not believe asset size of an organization should impact its obligation to notify regulators of a "notification incident."

Question 4: Is the proposed requirement that banking organizations and bank service providers notify the appropriate party when they "believe in good faith" that they are experiencing or have experienced a notification incident or computer-security incident, as applicable, sufficiently clear such that banking organizations and bank service providers understand when they should provide notice? How should the "believes in good faith" standard be modified, if at all? For example, should the standard be "reasonably believes" for either banking organizations or bank service providers?

As we have discussed, we do not believe that "believe in good faith" is the appropriate threshold and trigger for the Proposal. Whether in the context of a "computer-security incident" or "notification incident," the tipping point for notification to regulators is when the banking organization determines that the former has risen to the status of the latter. Importantly, a *determination* is a much clearer threshold, whereas a "belief in good faith" is arguably more subjective and uncertain and could lead to delays in notification.

Question 9: Do existing contracts between banking organizations and bank service providers already have provisions that would allow banking organizations to meet the proposed notification incident requirements?

Generally, yes. Coalition members engage service providers for many reasons and to perform many different tasks, from core operations to information technology and human resources. In all cases, contracts between parties are detailed and explicit in delineating responsibilities, including those necessary to meet regulatory and legal obligations. For example, to comply with the 50 different state data breach notification requirements, contracts routinely address roles and duties between a service provider acting as an agent to

the principal insurance company. That said, there will likely be instances where contractual terms would need to be modified to address the particular elements of the Proposal.

Question 10: Does the definition of "bank service provider" in the proposed rule appropriately capture the services about which banking organizations should be informed in the event of disruptions? Should all the services included in the Bank Service Company Act be included for purposes of banking organizations receiving notice of disruptions from their bank service providers? If not, which services should require a bank service provider to notify its affected banking organization customers when those services are disrupted, and why? Should the requirement only attach to a subset of services provided to banking organizations under the BSCA or should it only attach to certain bank service providers, such as those that are examined by the federal banking agencies?

Generally, we believe contracts should dictate the criteria for notification between banking organizations and service providers, not regulation. Since the Proposal places the burden of regulatory notification on the banking organization in all cases, this point is made more acute.

Further, the Proposal states that a bank service provider is required to notify affected banking organization customers "immediately after experiencing a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the BSCA for four or more hours." Here, we offer two comments: First, we believe banking organizations are best positioned to know which of their service providers provide services relevant to the covered situations that would warrant notification, and as such, the rule does not need further detail in this regard. Second, as we have stated in response to previous questions, we recommend that the threshold for notification by a service provider to its banking organization customers be the *determination* the service provider makes that a "computer-security incident" has or may have occurred, and that the concept of "impairment" be dropped as redundant. Thus, the requirement should state:

A bank service provider that provides a service described under the BSCA shall notify at least two individuals at affected banking organization customers immediately upon determining that a computer-security incident that could disrupt or degrade services provided subject to the BSCA for four or more hours has or may have occurred.

Question 12: Within what timeframe should bank service providers provide notification to banking organizations? Is immediate notification after experiencing a disruption in services provided to affected banking organization customers and to report to those organizations reasonable? If not, what is the appropriate amount of time for a bank service provider to determine it has experienced a material disruption in service that impacts its banking organization customers, and why?

We believe "immediate" notification by a bank service provider after experiencing a disruption is appropriate. However, as discussed in response to Question 10, we recommend that the threshold for notification by a service provider to its banking organization customers be the *determination* the service provider makes that a "computer-security incident" has or may have occurred, and that the concept of "impairment" be dropped as redundant. Thus, once a bank

service provider determines that a “computer-security” incident has or may have occurred, immediate notification to banking organization customers is required.

As we also discussed, any additional requirements regarding notification between bank service providers and banking organizations should be resolved via contract.

Question 14: Describe circumstances in which a bank service provider would become aware of a material disruption that could be a notification incident for banking organization customers but the banking organization customers would not be aware of the incident. Would it be overly burdensome to certain bank service providers, such as smaller bank service providers, to provide notice of material disruptions, degradations, or impairments to their affected banking organization customers and, if so, why?

Coalition members, and we believe banking organizations generally, would be very unlikely to enter into a business arrangement with a service provider that could not meet a regulatory requirement such as that contained in the Proposal. It would not be acceptable, nor likely would it be permitted contractually, for a bank service provider to escape notification requirements to its banking organization customers simply because it is small.

Again, thank you for the opportunity to provide these comments and we appreciate your consideration of our views. We would be pleased to engage in further discussion on these matters as the agencies move forward with this proposal.

Sincerely,

Bridget Hagan
Executive Director, The Insurance Coalition