Monday, April 12, 2021

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

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

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 (OCC)

Submitted electrically: *regs.comments@federalreserve.gov*
comments@fdic.gov
www.regulations.gov

Attention: Comments (FDIC)
Comment Processing (OCC)

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)

Dear Sir or Madam:

The Ohio Bankers League (OBL)[1] appreciates the opportunity to provide comments in response to the January 2021 notice of proposed rulemaking, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* ("Proposal"), jointly issued by the Federal Reserve Board of Governors, the Office of the Comptroller of the Currency, and the

[1] The Ohio Bankers League ["OBL"] is a non-profit trade association that represents the interests of Ohio's commercial banks, savings banks, savings associations as well as their holding companies and affiliated organizations. The Ohio Bankers League has over 170 members which represents the overwhelming majority of all FDIC insured depository institutions doing business in this state. OBL membership represents the full spectrum of FDIC insured depository institutions from small mutual savings associations owned by their depositors, community banks that are the quintessential locally-owned and operated businesses, up to large regional and multistate holding companies that have several bank and non-bank affiliates and conduct business from coast to coast. Ohio depository institutions directly employ more than 70,000 people in Ohio. We are the only trade association in Ohio that represents all segments of FDIC insured depository institutions. www.ohiobankersleague.com

Federal Deposit Insurance Corporation ("Agencies"). On behalf of our members, we look forward to facilitating a constructive dialogue between the Agencies and the banking industry to develop a notification framework that provides the timely notice of disruptions to the Agencies while not overburdening the banks we represent. Critical in this discussion is ensuring that there is a balance between providing the appropriate information when necessary while avoiding overreporting that has the potential to inundate both the regulators and the regulated.

Generally, OBL, on behalf of our members, believes the proposal can be improved to achieve the overarching goals in two broad ways—when reporting is required and how reporting is made. Further, there will likely be additional need to update the proposal in the future as the industry and service providers change.

The Proposal Requires Clarification to Avoid Overreporting and to Conform with Stated Intent

As currently drafted, the proposal lacks enough specificity to know when and how to report a computer-security incident and when such incident would rise to the level of a notification incident. This has the potential to lead to overreporting to the Agencies to avoid missing an event that could later be deemed as reportable. Overreporting is detrimental to both the Agencies and banks because it strains staff at the bank to make the report, when it may not be necessary to achieve the stated goals, and the staff at the Agencies in reviewing what could be reviewed as the reporting of mundane events that do not rise to the appropriate level. This frustrates the stated goals of only seeking information on events that result in actual or extreme likelihood of harm or disruption.

To remedy this issue and cut down on the likelihood over the overreporting of incidents that do not rise to the level of having a deleterious effect on banking organization operations, OBL recommends that the proposal be modified in the following ways. First, the definition of computer-security incident should only include an occurrence that results in "actual" harm rather than "actual or potential" harm as included in the proposal. This removes much of the guesswork for bank employees in determining what types of occurrences could result in "potential" harm. To aid in this, the examples provided in the Proposal should be further clarified to provide additional guidance to banks on what needs to be reported.

Second, the definition of "notification" incident should be modified to replace the term "believe in good faith" with "determined" to ensure that only the most significant and potentially problematic computer-security incidents are reported to the Agencies. This is a more concrete standard that also provides the time necessary to properly evaluate whether a computer-security incident rises to the level outlined in the proposal to be reported.

Incorporation of Clear Communication Methods and Requirements

One of the goals of the Proposal is to provide the Agencies with early notice of significant computer-security incidents. As such, the Proposal states that the notification "is not intended include an assessment of the incident" which is critical to the 36-hour notice requirement being workable. It can take significantly longer to have a complete picture of a complex computer-security incident and to provide a complete assessment of the situation. This must be clearly articulated in the rule. Additionally, the rule should permit banking organizations to provide notice to Agencies through existing and commonly used communication channels. This will allow for straightforward reporting during what can be extremely trying times at institutions of all sizes.

Inclusion of Bank Service Provider Notification Requirements

OBL members appreciate the recognition that bank service providers play a key role in financial institutions' daily operations and requiring those providers to notify banks of computer-security incidents is critical to banks' ability to mitigate and provide notice to the Agencies. This helps to balance any real or perceived inequities in negotiating power with some bank service providers to demand certain contractual provisions that would require this type of notice. However, these provisions may take time to fully incorporate into all the service provider contracts currently in existence as those contracts come up for renewal. It should also be clearly stated in the rule, as it has been articulated in the Proposal, that banks will not be cited for the failure of a service provider to comply with the rule.

Conclusion

On behalf of OBL members, we appreciate the ability to provide comments on this important rule. Please contact me with any questions about the comments contained in this letter.

Sincerely,

Don Boyd
VP, State Government Relations & General Counsel