April 12, 2021

Mr. James P. Sheesley
Assistant Executive Secretary

Attention: Cross River Bank's Comment Letter Regarding Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

Federal Deposit Insurance Corporation (FDIC)
550 17th Street, N.W.
Washington, D.C., 20429

Re: ***"Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers"***
RIN 3064-AF59

Dear Mr. Sheesley,

On behalf of Cross River Bank ("Cross River" or the "Bank"), I thank you for the opportunity to provide comments on the Federal Deposit Insurance Corporation's ("FDIC" or the "Agency") Notice of Proposed Rulemaking ("NPR") entitled, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers." Cross River applauds the joint efforts of the prudential regulators to implement a uniform regulatory standard aimed at protecting the security of the financial system.

Cross River is a New Jersey State chartered, FDIC insured financial institution that merges the trust and reliability of a community bank with the innovative offerings of a technology company. Since inception, the Bank has consistently partnered with leading technology companies to offer a suite of products that empower consumers to take control of their financial health by facilitating access to affordable credit in a responsible manner.

Cross River fully appreciates the responsibilities associated with being a regulated financial institution and the Bank's role in protecting the integrity of the financial system. Key to the Bank's commitment to upholding a best in class regulatory and compliance framework is transparent coordination with all applicable regulatory agencies. Open lines of communication between the industry and regulatory agencies are paramount to a frictionless and successful regulatory system. Cross River applauds the FDIC and other Agencies' efforts to create a uniform standard regarding reporting in the event of a computer security incident.

Cross River strongly supports the Agencies' efforts to create a harmonious standard that minimizes regulatory burden and ensures the safety of both consumers and the financial system as a whole. In an effort to achieve the Agencies' underlying goal of creating a more secure and stable financial system without creating over burdensome protocols, Cross River recommends certain amendments and clarifications be added to the proposed rule. Specifically, the Bank recommends:

1. The definition of "computer-security incident" should be amended to include only incidents that result in actual harm;
2. The definition of "notification incident" should be further tailored to ensure the rule does not exceed its intended scope and does not create an abundance of unnecessary reporting requirements;
3. The proposed 36 hour reporting requirement should be extended to 72 hours to allow financial institutions to adequately assess potential incidents; and
4. The notification requirement should be simple, concise and flexible, utilizing existing communication channels.

These recommendations will ensure that the Agencies' have appropriate notice of potential threats and the tools to combat them without overburdening financial institutions or creating an abundance of unnecessary reporting.

Discussion of Comments on the Propose Rule

1. The definition of "computer-security incident" should be amended to include only incidents that result in actual harm.

The proposed rule defines "computer-security incident" as "an occurrence that: (1) 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 (2) Constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."[1]

The existing definition captures and overly broad number of occurrences that may rise to a level of a notification incident without producing any harm whatsoever to the financial system itself. To narrow the scope of this definition and create a more effective, efficient, and meaningful standard, an incident should only be triggered when actual harm has occurred.

If the scope of the definition is not limited, the final rule will create burdensome requirements for financial institutions. This could potentially inundate the Agencies' as they would have to review each notice, despite the majority of them having no effect on the safety or soundness of the financial system. Tailoring the definition of both the terms "computer-security incident" and "notification incident" will help to create a manageable standard consistent with the Agencies' mission of protecting the financial system.

2. The definition of "notification incident" should be further tailored to ensure the rule does not exceed its intended scope and does not create an abundance of unnecessary reporting requirements.

The proposed rule defines "notification incident" as,

[1] Proposed section 53.2(b)(4), 86 Fed. Reg. at 2309; Proposed section 225.301(a), 86 Fed. Reg. at 2310; Proposed section 304.22(b)(4) at 86 Fed. Reg. 2311.

> "a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair: (i) The ability of the banking organization 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; (ii) Any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or (iii) Those operations of a banking organization, 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.[2]

While Cross River supports the goals and purpose of this proposed definition, the Bank believes that as written, the definition creates an overly broad scope that would result, contrary to the Agencies' intention, in a significant compliance burden on banking organizations in the form of over-reporting of less significant or easily remediated events. In order to better achieve the Agencies' goal of minimizing regulatory burdens that are likely to cause significant harm, Cross River recommends the definition of "notification incident" be revised to read,

> "A notification incident is a 'computer-security incident' that (a) results in ***actual harm*** to an information system that carries out banking operations, activities, or processes, or delivers banking products or services in the ordinary course of business; and (b) a banking organization determines in good faith **is reasonably likely** to materially disrupt, degrade, or impair—(i) The ability of the banking organization 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; (ii) Any business line of a banking organization, including associated operations, services, functions and support, and would result, on an enterprise basis, in a material loss of revenue, profit, or franchise value; or (iii) Those operations of a banking organization, 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."

Narrowing the scope of the definition, so as to only be triggered when actual harm occurs will help to achieve the Agencies' mission of preventing wide spread harm while simultaneously minimizing the burden institutions would face from needing to communicate events that have no baring on the financial system. Removing the term "could" and replacing it with "is reasonably likely" creates a more definitive and clearer standard removing ambiguities. This definitive language will help provide assurances to financial institutions and help ensure they are fully complying with the spirit of the rule.

This tailored definition will help to ensure financial institutions are not overly burdened and do not incur unnecessary expenses, while fully protecting the security of the financial system. Under this amended definition, the Agencies will be informed of all incidents that raise to the level the proposed rule intended to capture without creating a complex, expensive or over overly burdensome framework for financial institutions to comply with.

3. *The proposed 36 hour notification requirement should be extended to 72 hours to allow financial institutions to adequately assess potential incidents.*

[2] Proposed section 53.2(b)(5), 86 Fed. Reg. at 2310; Proposed section 225.301(a), 86 Fed. Reg. at 2310; Proposed section 304.22(b)(5) at 86 Fed. Reg. 2311.

Cross River understands the necessity for a prompt and timely reporting response in the event of a cyber security incident. Transparency and collaboration during these times may help to prevent further attacks or larger scale harm to the financial system as a whole. However, as currently written, the prescribed 36 hour notification requirement does not allow financial institutions, especially smaller community banks, to adequately assess if there has in fact been an incident worthy of reporting.

The Bank appreciates that the Agencies have recognized this internal process may be tedious, take banking organizations a reasonable amount of time to conduct and "do not expect that a banking organization would typically be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident."[3] The internal process and procedures that are conducted in the event of a suspected incident are both complex and time consuming. For community banks especially, and smaller institutions that do not have an unlimited amount of resources, this process can take extended periods of time to ensure a thorough examination of the events have occurred. Often because of these factors it may not be possible to determine in good faith that an event has occurred within the proposed 36 hour timeframe.

To best fulfill the intent of the proposed rule and create a standard that all institutions, regardless of size or resources, will be able to effectively comply with, Cross River recommends the Agencies' amend the proposed rule to require, "a banking organization to notify its primary federal regulator of any computer security incident that rises to the level of a notification incident as soon as ***practicable*** and no later than ***72*** hours after the banking organization believes in good faith that a notification incident has occurred." As currently written in the preamble of the proposed rule, the Agencies would require notification as soon as possible and no later than 36 hours.

As described above, Cross River believes that the Bank's proposed standard would adequately address the Agencies' concerns and intention of creating a timely notification requirement while allowing financial institutions to thoroughly complete their own internal process and evaluations. The term "practicable," in our view, better captures that concept, avoiding any misperception that because one organization was able to conclude in a particular timeframe that a notification incident has occurred, it was "possible" that other organizations could have done so as well. The extension to 72 hours would ensure that institutions of all sizes had the capacity to adequately assess potential incidents.

Additionally, increasing the requirement to a 72 hour notice period would better account for federal holidays, weekends and other occasions where offices may have reduced capacity. Specifications as to whether the requirement would be triggered according to business or calendar days would be of further assistance in ensuring a clear standard is implemented.

These recommendations are consistent with the Agencies' overall mission of protecting the financial system from potential harm and give financial institutions the ability to more effectively communicate with the Agencies' about any potential harms and real threats.

[3] *See* 86 Fed. Reg. at 2302 and 2303 ("The Agencies recognize that a banking organization may be working expeditiously to resolve the notification incident—either directly or through a bank service provider—at the time it would be expected to notify its primary federal regulator.").

4. *The notification requirement should be simple, concise, and flexible, utilizing existing communication channels.*

Cross River supports the Agencies' efforts and intention to create a flexible notice procedure. The development of such a procedure should be administered through existing communication channels and provide concise instructions. Key to the success of this proposed rule is a simple notice procedure that allows financial institutions flexibility in choosing how the give notice of these events.

Conclusion

Cross River supports the Agencies' efforts to create a uniform security standard across the industry in order to protect the financial system. As the industry continues to undergo a digital transformation, it is important the regulations in place help to mitigate any forms of cyber risk.

Cross River believes that the recommendations provided in this letter will help to ensure the security of the industry without over burdening financial institutions. The proposed changes will help to ensure financial institutions have the appropriate time and tools to examine and mitigate any potential risks without overflowing the Agencies' with unnecessary reporting information.

The Bank welcomes the opportunity to continue to collaborate with the Agencies' and serve as a partner in combating risks posed to the financial system. Transparency, communication and coordination between industry and regulators is essential to the success of this proposed rule.

If you have any additional questions, please do not hesitate to contact Arlen Gelbard, *EVP*, General Counsel at agelbard@crossriverbank.com or 201-808-7189. We look forward to continuing engaging in dialogue and serving as a resource for the Agency in the future.

Best,

Aaron Iovine
Head of Policy and Regulatory Affairs