COMPLIANCE COMMITTEE

PATRICK T. CAMPBELL
CHAIR
pcampbell@bakerlaw.com

ADAM FELSENTHAL
SECRETARY
afelsenthal@gppfunds.com

April 12, 2021

Via Electronic Submission

Re: RIN 1557-AF02 (OCC), 7100-AF (Board), 3064-AF59 (FDIC); Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers; Docket ID OCC-2020-0038

The New York City Bar Association's Compliance Committee (the "Compliance Committee") submits this letter in response to the request of the Office of the Comptroller of the Currency, the Board of the Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (together, the "Agencies") for comment about the Notice of Proposed Rulemaking (the "Proposed Rule" or "Proposal") published on January 12, 2021. The Proposal seeks to require a banking organization to provide its primary federal regulator with prompt notification of any significant "computer-security incident" that could jeopardize the viability of its operations, which the Proposal refers to as a "notification incident." The Compliance Committee has a diverse membership that includes attorneys from law firms, in-house counsel, compliance professionals at various financial institutions, as well as representatives of regulatory and governmental agencies.

I. SUMMARY

At the outset, the Compliance Committee notes that it supports the Agencies' stated objectives for the Proposed Rule, which include providing the Agencies with earlier awareness of cybersecurity incidents that may so severely impact a banking organization that it can no longer support its customers and could impact its safety and soundness, leading to its failure. The sooner the Agencies know of a cybersecurity event, the better they can assess the extent of the threat and take appropriate action; provide information to a banking organization that may

not have previously faced a particular type of notification incident; and conduct analyses across supervised banking organizations to improve guidance, adjust supervisory programs, and provide information to the industry to help banking organizations protect themselves.

The Compliance Committee shares the Agencies' concern about the unique threats the current cyber risk landscape poses for the banking industry, including the increasing reliance by banking organizations on bank service providers to provide essential technology-related products and services. The Compliance Committee also recognizes that notification regimes currently required under the Gramm-Leach-Bliley Act and the Bank Secrecy Act do not provide the Agencies with information on cyber incidents affecting banking organization operations more broadly.

The Compliance Committee concurs that early notice to regulators is of critical importance. Regulators are the monitors of banking organization safety and soundness and should be informed of material security events and remedial efforts being undertaken. In addition, the provision of prompt notice is critical for regulators to monitor the banking sector and evaluate overall threats thereto. The SolarWinds attack demonstrates the importance of notice – numerous interrelated private and public entities and their third parties were compromised by a nation state actor. The breadth of this attack demonstrates the need for regulators to be informed and help ensure best practices are being applied throughout the regulated community to address the risks.

Most bank organizations have compliance programs in place to address information security, incident response, business continuity, and vendor management and to periodically test these programs through risk assessments and tabletop exercises. However, aspects of the Proposed Rule, specifically the definitions and materiality of reportable security incidents, will present an increased compliance burden for banking organizations, while providing the Agencies with notice of far too many security incidents that, at 36 hours out, could, but may not ultimately, have a significant impact on operations. The Compliance Committee makes the following recommendations to limit the notification requirement to high-threshold cybersecurity incidents that materially impact operations. As amended, the Proposed Rule will provide opportunity for bank organizations to continue to enhance their risk assessment practices and governance via a reevaluation and updating of their incident response, business continuity, and vendor risk management programs, while providing the Agencies with meaningful information to manage cyber threat risks that better aligns with their stated objectives in the Proposed Rule.

The Agencies seek comments on "all aspects of their proposal" and specifically on 16 questions. This letter provides comments on the following issues covered by five questions: (i) applicable definitions and standards triggering the notice requirement (questions 1, 2, 4 and 15), and (ii) the form and method of notice (question 5).

II. THE COMPLIANCE COMMITTEE'S COMMENTS TO THE PROPOSED RULE

A. Proposed Definitions and Standards

Questions 1 and 2 inquire how the definitions of "computer-security incident" and "notification incident" should be modified, if at all. Question 4 asks whether the "believe in good faith" standard is sufficiently clear.

The Proposed Rule would define 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.*

Defining computer-security incident to include potential harm is a definition that is common and appropriate for the scope of a cybersecurity program. Of course, it is critical to create a program to defend against potential threats and a good cybersecurity program will analyze threats that have been and that could be impactful on an organization. That would include both the threats that have been initiated against a particular organization and those that are being seen in the market at large. In addition, as proposed by the rule, it is appropriate for a bank service provider to be required to alert a banking institution to foreseeable threats and outages.[1] However, as described below, the definition of computer-security incident for purposes of regulatory notice should be narrower.

The Proposed Rule would define 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 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;*
> >
> > *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*
> >
> > *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 U.S.*

[1] This comment letter does not take a position regarding the required notice bank service providers should provide to banking organizations either by rule or by contract. Such relationships can be critical to the financial infrastructure and are often factually distinct.

As soon as possible and no later than 36 hours after a banking organization believes in good faith that it has experienced a computer-security incident that rises to the level of a notification incident, the Proposal would require the banking organization to notify its primary regulator.

In response, the Compliance Committee recommends that the definition of computer-security incident for regulatory notice purposes be modified to be limited to an occurrence that results in **actual harm** to applicable information and systems, or that results in **actual violation** of applicable security policies. The Compliance Committee also recommends that the definition of notification incident be modified to apply to a computer-security incident the banking organization "believes in good faith **has** materially disrupted, degraded or impaired" its operations, revenues or wider financial sector stability. Limiting regulatory notification to incidents that have materially harmed or violated the security of an organization meets the stated objectives of the Proposed Rule to provide the Agencies with early alert of significant, high-threshold security incidents so that the Agencies can assist the impacted organization to respond and recover as well as provide the Agencies with insight for taking action to bolster the wider sector.

Unfortunately, cybersecurity threats against financial institutions are occurring with significant frequency. A fulsome cybersecurity program must constantly be following threats and threat intelligence and analyzing potential threats against the organization to improve systems and its defensive posture. Organizations routinely acquire threat intelligence information from a variety of sources for their cybersecurity programs and actual threats against the organization are just a part of its threat intelligence analysis. However, analyzing threat intelligence for purposes of reporting it to regulators would add an unnecessary layer to the evaluative process that could take time and energy away from protective operations and would result in notifications to regulators beyond the intended purpose of the Proposed Rule. Reporting to regulators actual, rather than potential, events is a sensible requirement to enable the regulator to have visibility into events that may threaten the safety and soundness of the institution. A regulator's review of a banking organization's overall evaluation and analysis of threats to the organization are better conducted in the context of an examination during which the regulator can observe the organization's threat evaluation process as a whole, rather than a point in time threat.

The Compliance Committee supports tying the "believes in good faith" subjective standard to an event that has actually occurred and materially impacted operations, revenues or wider financial stability. It is appropriate to include a materiality standard as there is no one-size-fits-all assessment of the seriousness of a cybersecurity attack. Different banking organizations have different capabilities and products and the likelihood of an event endangering safety and soundness will differ for different institutions. That evaluation is best made by the banking organization and there is no regulatory benefit to second guessing an organization's good faith judgment. The Compliance Committee supports the risk-based rather than one-size-fits-all approach.

The Compliance Committee notes that the Proposed Rule's 36 hour notification requirement is substantially shorter than the 72 hour notification requirements under the EU's

General Data Protection Regulation and the New York State Department of Financial Services requirement under its cybersecurity regulation.[2] Given the compliance burdens posed in meeting varied timeframe reporting requirements, the Agencies should consider the universe of banking organizations that would be subject to these varied requirements in determining an appropriate and streamlined advance notification timeframe.

Question 15 invites comment on specific examples of computer-security incidents that should, or should not, constitute notification incidents. The Committee reviewed the proposed non-exhaustive list of "notification incidents" under the revised definitions in its response to Question 1 and 2, above, to determine if they rise to the level of "actual harm," "actual violation," or an incident that "has" occurred. Some proposed "notifications incidents" as drafted do not meet those standards. Specifically, the use of subjective periods of time, e.g., "undeterminable" and "extended period of time" outlined in incidents 2 and 5, respectively, do not provide sufficient guidance on whether a notification incident would rise to the level of an actual harm or violation of security standards. The Compliance Committee appreciates the clarity provided by incident 1 with respect to a defined time period, i.e., "more than 4 hours." It is recommended that an objective timeframe be established for all incidents that include a time period element. Additionally, the Committee finds that incident 7 is captured by incident 2 and/or is duplicative of various federal and state breach notification laws.

B. Proposed Method of Notifying the Agencies

Question 5 asks how banking organization notification should be provided to the Agencies. According to the Proposed Rule, a banking organization only needs to share general information about what is known at the time and does not prescribe the contents to be included in the notice nor any particular format – "any form of written or oral communication, via email or phone, to a designated point of contact identified by the Agencies is sufficient."

The Compliance Committee agrees that the contents of the notification provided to the Agencies not be prescribed; however, to reduce the compliance burden for banking organizations, the Compliance Committee urges the Agencies to adopt an easy-to-follow, streamlined, and secure form and method of notifying the Agencies. Given that the notification is meant to serve only as an early alert to regulators and is not intended to provide any "assessment of the incident," the Compliance Committee supports creation of a form and method of notice that is streamlined across the Agencies via a highly secure delivery system to protect the extremely sensitive notification being conveyed. The Compliance Committee also recommends that any form of notice and delivery system be optional and not mandatory given that security incidents impact organizations in different ways, and in some cases may interfere with access to the particular system provided for notice. In such cases, organizations should not be penalized for failing to use a particular system so long as good faith notice is made.

[2] Regulation (EU) 2016/679 (General Data Protection Regulation); 23 NYCRR Part 500.

* * *

The Compliance Committee appreciates the opportunity to comment on the Proposed Rule. If we can be of further assistance in this regard, please feel free to contact us.

Respectfully submitted,

Patrick T. Campbell
Chair, Compliance Committee

Drafting Subcommittee:

Heather McArn
Samara Yousif
Andrew Tobel
Michael Savicki