Banking Agencies Propose Cyber Reporting Rule: Implications for Cybersecurity Compliance

December 22, 2020

On December 15, 2020, the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Federal Deposit Insurance Corporation (the Banking Agencies) issued a **notice of proposed rulemaking** (the Proposed Rule) that would require substantially faster notification of cybersecurity incidents involving banking organizations,[1] expand the list of triggering events, and impose first-of-its kind notification requirements for bank service providers. Banking organizations and their service providers should consider reviewing their incident response plans for compliance with the Proposed Rule and should consider commenting on the proposal. Comments are due 90 days after publication in the Federal Register, which is expected soon.

Key Features of the Proposed Rule and Differences with Existing Regulations

- ***36-Hour Notification Deadline.*** Banking organizations would be required to notify their primary federal regulators within 36 hours of identifying a "computer-security incident" that rises to the level of a "notification incident."

    - Existing federal cyber incident disclosure requirements, the Gramm-Leach-Bliley Act and its Security Guidelines (GLBA) and the Bank Secrecy Act (BSA), allow more time to provide disclosure. The GLBA requires reporting of covered incidents "as soon as possible," and the BSA allows up to 30 days to develop and file a Suspicious Activity Report (SAR).

- ***Broad Definition of Computer-Security Incident.*** This term would encompass an incident that (i) 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 (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

    - The Proposed Rule goes further than the GLBA or the BSA, defining computer-security incidents to include service disruptions. For example, a failed system upgrade or change that results in widespread user outages for customers and bank employees would likely be considered a "computer-security incident" and, if it is a "notification incident," would need to be disclosed. By contrast, the **2005 Interagency Guidance for the GLBA** concerns incidents "involving unauthorized access to or use of sensitive customer information." Similarly, **FinCEN's 2016 directive** requires entities to file SARs in connection with cyber-events and cyber-enabled crime.

- ***Notification for Incidents that Could be Material.*** A computer-security incident becomes a "notification incident" if a banking organization "believes in good faith [the incident] 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

[1] Banking organization is a broad concept which includes national banks, savings associations, state-chartered banks, and any holding company of these institutions. This term also encompasses foreign branches of U.S. organizations and the U.S. operations of foreign banks. Credit unions are not included.

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."

  - The requirement that the "computer-security incident" rise to the level of a "notification incident" in order to trigger disclosure would require banking organizations to scrutinize their material cyber risks. The Banking Agencies estimate 150 such notification incidents across all regulated entities per year. The figure is based on their review of indicative descriptors (e.g., ransomware, trojan, zero day) in supervisory data and cyber-related SARs, though their descriptor list may be undercounting non-threat actor incidents.

- ***Notification by Bank Service Providers*.** For the first time ever, the Proposed Rule would require bank service providers to immediately notify at least two employees at customer banks of any computer-security incident that could "disrupt, degrade, or impair" provider services for four or more hours. A "bank service provider" would include "bank service companies" and third-party providers under the Bank Service Company Act.

Additional Implications for DFS-Regulated and Publicly Traded Banking Organizations

The New York Department of Financial Services (DFS) Cybersecurity Regulations **23 NYCRR 500** require a bank chartered in New York, or any other organization licensed by the DFS, to notify the DFS no later than 72 hours after determining that it has experienced a "cybersecurity event." Although the DFS's "cybersecurity event" differs from the Proposed Rules' "notification incident," a cybersecurity incident that materially affects the bank's operations may trigger requirements under both laws. Moreover, the DFS requires notice of any cybersecurity event that requires notice "to be provided to any government body, self-regulatory agency or any other supervisory body" further increasing the prospect that notification under the Proposed Rule would trigger DFS notification.

The Proposed Rule's requirement that banking organizations disclose any incident that *could materially* impact the business may also have disclosure implications for public companies. The SEC has repeatedly emphasized in recent years the need for fulsome disclosure of material cybersecurity incidents in securities filings—including in its **2018 interpretive guidance**. Public banking organizations would need to carefully consider whether an event that triggers notification under the Proposed Rule also constitutes a material cyber incident for which the SEC would expect disclosure in quarterly or annual reporting—or even in an 8-K or 6-K depending on the materiality of the incident to investors.

How to Respond

To address the implications of the Proposed Rule banking organizations should consider:

- Reviewing incident response procedures, and conducting tabletop exercises, to ensure the organization can:

  - Identify and assess the materiality of "computer-security incidents" at the organization and at its service providers.

  - Execute notification to applicable Banking Agencies within 36 hours of identifying a "notification incident."

  - Determine where notification under the Proposed Rule would trigger related reporting obligations—and how to meet those obligations.

- Providing comments on the Proposed Rule, which are due within 90 days of its publication in the Federal Register. The Banking Agencies specifically seek input on:
    - The definitions of "computer-security incident" and "notification incident."
    - The estimated number of notification incidents.
    - Whether to adjust the 36-hour notification timeline.
    - The propriety of the "good faith" standard for determining whether an incident requires notification.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres	+1 212 450 4724	**greg.andres@davispolk.com**
Robert A. Cohen	+1 202 962 7047	**robert.cohen@davispolk.com**
Gabriel D. Rosenberg	+1 212 450 4537	**gabriel.rosenberg@davispolk.com**
Margaret E. Tahyar	+1 212 450 4379	**margaret.tahyar@davispolk.com**
Matthew J. Bacal	+1 212 450 4790	**matthew.bacal@davispolk.com**
Daniel F. Forester	+1 212 450 3072	**daniel.forester@davispolk.com**
Matthew A. Kelly	+1 212 450 4903	**matthew.kelly@davispolk.com**
Will Schildknecht	+1 212 450 3557	**will.schildknecht@davispolk.com**