CLIENT ALERT

Newly Proposed Cyber Reporting Rules for Banking Organizations

Feb.01.2021

Last month, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (the Board), and the Federal Deposit Insurance Company (FDIC) issued a Notice of Proposed Rulemaking (86 F.R. 2299) that would require notification from banking organizations and their service providers within 36 hours of the discovery of a broad array of cybersecurity incidents that could "materially disrupt, degrade, or impair" banking operations.

The rule would fill a gap among current federal regulations—including the Bank Secrecy Act (BSA), the Gramm-Leach-Bliley Act (GLBA), and the Bank Service Company Act (BSCA)—which at present do not impose direct cybersecurity incident reporting requirements with defined deadlines on banking organizations. The federal banking authorities' *Interagency Guidelines Establishing Information Security*, first published in 2001, do implement sections 501 and 505(b) of the GLBA to require that a banking organization notify "its primary federal regulator *as soon as possible* when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information" (emphasis added); however, the guidelines do not impose a specific deadline for such notification, nor do they offer detailed (or updated) definitions of incidents involving either "unauthorized access" or "sensitive customer information." The Securities and Exchange Commission (SEC) has also published its 2018 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Release Nos. 33-10459; 34-82746), which outlines the cybersecurity incident disclosure requirements public operating companies must meet in their registration statements—though as with the *Interagency Guidelines*, the substance and timing of these disclosures weighs heavily on companies' own judgment. Similarly, while certain banking organizations are required to file Suspicious Activity Reports (SARs) when they become aware of a violation of federal criminal law or a suspicious activity related to money laundering, those reports may be filed within 30 days. Notwithstanding the existing landscape, the proposed rule seeks to broaden the types of cybersecurity incidents that must be reported and improve timely notice of such incidents.

In particular, the proposed rule would require any banking organization that experiences a "computer-security incident" that meets the rule's threshold of a "notification incident" to report such an occurrence to the organization's primary federal regulator no later than 36 hours after the organization "believes in good faith that a notification incident has occurred." The rule also would require that banking service providers (as defined under the BSCA[1]) notify at least two individuals at affected banking organizations upon "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."

The proposed rule defines "computer-security incident" broadly to include those involving both actual and "potential" harm, as well as unauthorized access. It also applies to all "information the [banking organization's information technology] system processes," not just personally identifiable information (PII). "Notification incident" is defined more narrowly in the proposed rule, encompassing only those incidents the banking organization believes in good faith "could materially disrupt, degrade, or impair" the organization's ability to carry out either core operations, operations which would result in material loss of revenue, or operations linked to the financial stability of the United States.

Many banking organizations may already have extant cybersecurity incident reporting policies roughly in line with the obligations of the proposed rule. Similar reporting requirements have been imposed on certain banking organizations at the state level, with, for example, the New York Department of Financial Services instituting a 72-hour reporting deadline on banking organizations that experience a cybersecurity incident. These obligations exist in addition to those generated by customer-centric data privacy regulations that have been adopted by most state legislatures in some form. Moreover, in recent years, banking organizations have actively included incident reporting language in their contracts with banking customers. Nevertheless, the 36-hour reporting requirement adopted by the proposed rule would be one of the strictest federal reporting deadlines for cybersecurity incidents.

The proposed rule requests comments on 16 specific questions by April 12, 2021. Those questions include whether the definitions of "computer-security incident" and "notification incident" should be modified; whether the timelines for reporting should be altered; and whether the 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 is sufficiently clear. Banking organizations and their service providers should review their existing cybersecurity incident disclosure policies and procedures, and consider the breadth and degree of changes to those policies and procedures that compliance with the proposed rule would require.

---

[1] The BSCA applies "banking service provider" to all vendors, including technology service providers, who engage in "check and deposit sorting and positing, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices and similar items, or any other clerical, bookkeeping, account, statistical, or similar functions" on the part of banking organizations. 12 U.S.C. § 1863.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Paul C. Mathis
Associate – Washington, D.C.

Phone: +1 202.688.3432
Email: pmathis@crowell.com