Update on Cybersecurity Breach Notification Requirements

Related Professionals

Matt K. Walker

Related Services

Corporate and Business Organizations

Related Industries

Financial Institutions

AUTHORED ARTICLE | Summer 2022

Published in the Summer 2022 issue of *The Bankers' Statement*

As cybersecurity concerns and threats continue to rise exponentially for banks of all sizes and types, the regulatory landscape is changing just as quickly. Within the last year alone, the federal banking agencies, the Securities and Exchange Commission (SEC), and Congress have all undertaken various rulemaking initiatives surrounding this topic, as described in greater detail below. Banks should closely monitor these initiatives as they unfold to better understand how each may affect their ongoing cybersecurity incident notification obligations.

Federal Banking Agencies

On November 23, 2021 the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), and the Federal Deposit Insurance Corporation (FDIC) published a final rule establishing computer-security incident notification requirements.[1] The rule applies equally to all banks and bank holding companies, including national banks, federal savings associations, state-chartered banks, bank holding companies, and savings and loan holding companies. Also, it's important to note that unlike some of the proposed rules discussed later in the article, this rule has already been finalized, with an effective compliance date of May 1, 2022.

The final rule requires banking organizations to promptly notify their primary federal regulator of any "computer-security incident" that raises to the level of a "notification incident." Any required notification must occur as soon as possible, but no later than 36 hours after a notification incident has occurred. A "notification incident" is generally defined by the rule to include a significant computer-security incident that disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the banking organization's operations, results in customers being unable to access their deposit and other accounts, or impact the stability of the financial sector. This may include a major computer-system failure; cyber-related interruption, such as a distributed denial of service or ransomware attack; or another type of significant operational interruption. The rule further defines a

"computer-security incident" as an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

A bank must provide this notification to its agency-designated point of contact (or as alternative for FDIC and OCC supervised banks, to that agency's respective supervisory office) through email, telephone, or other similar methods that may be prescribed.

The rule separately requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours. The required notification must be made to a bank-designated point of contact or, if one has not been provided, to the bank's CEO and CIO.

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)

CIRCIA was included as part of the 2022 federal omnibus appropriations bill, which President Biden signed into law on March 15, 2022. The legislation[2] will require "covered entities" to report a "covered cyber incident" to the U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) within 72 hours after it reasonably believes the incident has occurred. Separate reporting to CISA is also required within 24 hours, if a ransom payment is made as a result of a ransomware attack.

The terms "covered entities", "covered cyber incident", along with many other relevant considerations, have yet to be fully defined, but the bill does identify certain critical infrastructure sectors within its purview, notably including financial services. "Cyber incident" is already defined, however, as "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system." The bill provides some examples of reportable covered cyber incidents, such as a disruption of operations or a substantial loss of confidentiality, but a more comprehensive list is to be developed through rulemaking.

It's important to note that CISA, the agency tasked with implementing the new law, must promulgate rules before any of the law's provisions become effective. The agency has up to 24 months to issue a notice of proposed rulemaking and has 18 months beyond that to issue a final rule. Beyond defining the specific entities subject to CIRCIA and the relevant types of cyber incidents, the bill requires rules be proposed to address other important details such as a clear description of the specific content to be included in incident and ransomware payment reports, preservation of records, submission procedures, and established deadlines for any required supplemental reporting.

Additionally, the bill clarifies that required reports are exempt from disclosure under the Freedom of Information Act and their submission is not considered a waiver of any privilege or protection, such as those applicable to trade secrets. Even more importantly, the bill further clarifies no private right of action can be maintained based solely upon a covered cyber incident or ransom payment report, nor can the reports form the basis for a regulatory enforcement action (outside of limited exceptions). Finally, the Act requires CISA and other federal agencies to take steps, including entering into interagency agreements, to harmonize any overlapping reporting requirements so as to avoid duplicative or burdensome requirements.

Proposed SEC Cybersecurity Rules

The most recent noteworthy development in this area is a March 9, 2022, rule proposal by the SEC setting forth a series of cybersecurity related disclosure and reporting requirements for public companies[3]. Per the SEC, the proposal is intended to provide standardized and timely disclosures to investors and other market participants such that they can assess the possible effects of a material cybersecurity incident. In part, the proposed rules would require public companies to do the following:

- *Cybersecurity incidents* – Companies would be required to disclose a material cybersecurity incident, and specified information pertaining to the incident, on form 8-K within four business days after the company determines it has experienced a *material* cybersecurity event. It's important to note the proposed rules do not provide companies with a reporting delay for ongoing internal or external investigations related to the incident, including those conducted by law enforcement. The proposed rules further require any material updates to cybersecurity incident information previously disclosed on a form 8-K, be provided periodically on forms 10-Q or 10-K.
- *Cybersecurity risk management, strategy, and governance* – The proposed rules would also require companies to disclose annually on form 10-K their policies and procedures, if any, to identify and manage cybersecurity risks and threats, including if such risks are considered as a part of business strategy, financial planning, and capital allocation. Furthermore, disclosure would also be required of a company's cybersecurity governance, including a board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant cybersecurity expertise of management, and management's role in implementing the company's cybersecurity policies, procedures, and strategies. The rules would also require annual disclosure of the existence of any board member with cybersecurity expertise, including a helpful clarification that any such disclosure does not impart on the board member any *additional* duty, obligation, or liability.

Takeaway

While the aforementioned rules and regulations are in various stages of review and approval, banks should closely track each one based on the potential applicability to their organization, with specific attention paid to the particular events triggering notification under each requirement. Also, if they've not done so, institutions would be wise to begin revising their cybersecurity policies and procedures, along with any relevant incident response plans, to take into account the new notification requirements of the federal banking regulators, as those rules became effective May 1, 2022. Due diligence reviews should also be conducted of any third-party service provider contracts to ensure such parties will be compliant with the third-party provisions of the new federal regulator notification rules.

Ideally, if all three of these rulemaking initiatives come to fruition, due consideration will be given to harmonizing any overlapping and redundant notifications requirements. Regardless, these rules reveal, unsurprisingly, that heightened regulatory expectations surrounding cybersecurity incident notification are here to stay and, accordingly, institutions should be prepared to demonstrate they have the appropriate governance, oversight, and risk management structure in place.

---

[1] FDIC: FIL-74-2021: Computer-Security Incident Notification Final Rule

[2] H.R.5440 - 117th Congress (2021-2022): Cyber Incident Reporting for Critical Infrastructure Act of 2021 | Congress.gov | Library of Congress

[3] SEC.gov | SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies