Banks Have 36 Hours to Report a Data Incident or Breach to Regulators Starting May 1, 2022

On Nov. 18, 2021, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation (FDIC) announced the approval of a final rule for computer-security incident notification requirements for the U.S. banking system. The final rule becomes effective on April 1, 2022 and requires compliance by May 1, 2022. Banking organizations[1] will be required to notify their primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident," ***as soon as possible***, but not later than ***36 hours*** after the banking organization determines that a notification incident has occurred. Significantly, the final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially affected or is reasonably likely to materially affect banking organization customers for four or more hours.

"Computer-Security Incident and "Notification Incident" Defined

The final rule provides the definitions for *computer-security incident* and *notification incident*. Under the rule, a *computer-security incident* is "an occurrence 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." *Notification incident* is defined as "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."

---

1 Banking organizations are defined to include national banks, federal savings associations, U.S. bank holding companies, savings and loan holding companies, state member banks, insured state nonmember banks, insured state savings associations, federal branches and agencies of foreign banks, and insured state-licensed branches of foreign banks.

Impact of Final Rule

The purpose of this final rule, which comes on the heels of a significant uptick in ransomware attacks and cyber-intrusions throughout the U.S., is to provide banking agencies with every opportunity to have truly "prompt" awareness of emerging threats and potential systemic cyber risks. The expectation is that this rule will provide the U.S. bank regulatory agencies with immediate notice of serious incidents affecting U.S. banking organizations to protect those bank customers and their accounts and other assets. In practicality, a banking organization's incident response plans and third-party risk management programs may need to be reviewed/revised to account for the immediacy required under this final rule.

If you have any question about the information presented in this memo, please contact Jessica L. Copeland, Dori K. Bailey, Hoda Moussa or any attorney in Bond's Cybersecurity and Data Privacy practice.

BOND SCHOENECK & KING ATTORNEYS