THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 38 No. 5 May 2022

THE BANKING AGENCIES' FINAL RULE ON COMPUTER-SECURITY INCIDENT NOTIFICATION REQUIREMENTS

Responding to the increasing frequency and severity of cyberattacks on the financial services industry, the federal banking agencies have issued a final rule regarding required notifications of such attacks. The authors discuss the rule in detail, beginning with the Agencies' stated goals and key definitions in the rule. They then turn to updating incident response plans for compliance, incident notification requirements, and issues surrounding service provider contacts and contracts.

By Avi Gesser, Johanna Skrzypczyk, Michael R. Roberts, Courtney Bradford Pike, and Andres Gutierrez *

On November 18, 2021, the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Reserve Board ("FRB" or "the Board") (collectively, "the Agencies") announced the approval of a final rule that imposes new requirements on banking organizations and bank service providers for certain cybersecurity incidents. The Agencies issued the *Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* ("Final Rule"), which went into effect on April 1, 2022 and requires banking organizations, as well as certain banking service providers, to comply by May 1, 2022. Importantly, on March 29, 2022, the Agencies each issued guidance to their supervisory institutions regarding logistics for notification.

This article discusses three key components of the Final Rule, specifically: (1) new considerations and requirements for notifiable computer-security incidents; (2) steps to take to update incident response plans ("IRPs"); and (3) issues to consider when reviewing service provider relationships, including relevant contacts and contractual obligations. The Final Rule offers an opportunity for banking organizations to refine and formalize their processes and communications regarding computer-security incidents.

IMPORTANT DEFINITIONS AND GOALS

The Agencies' Goals and Considerations

The Agencies explained that they issued the Final Rule due to the increasing frequency and severity of cyberattacks in the financial services industry. Cyberattacks can harm banking organizations' networks, data, and systems, and impair their ability to carry out normal operations, such as providing customers access to their accounts. Some of the existing notification requirements, according to the Agencies, were not

**AVI GESSER is a partner, JOHANNA SKRZYPCZYK is counsel, and MICHAEL R. ROBERTS, COURTNEY BRADFORD PIKE, and ANDRES GUTIERREZ are associates at Debevoise & Plimpton LLP's New York City office. Their e-mail addresses are agesser@debevoise.com, jnskrzypczyk@debevoise.com, mrroberts@debevoise.com, cbpike@debevoise.com, and asgutierrez@debevoise.com.*