Banks would have 36 hours to report cyberattacks under proposed rules

AB americanbanker.com/news/banks-would-have-36-hours-to-report-cyberattacks-under-proposed-rules

By Paul Davis December 15, 2020

By Kevin Wack December 15, 2020, 4:05 p.m. EST 3 Min Read
New federal rules proposed Tuesday would require U.S. banks to notify their regulators about major computer security incidents within 36 hours.

If the rules are enacted, they would cover sophisticated criminal attacks and failed system upgrades, and would provide a hard near-term deadline where none currently exists. Still, government officials said that the proposal is tailored narrowly. They estimated that it would apply to only approximately 150 cyber incidents per year.

The Federal Deposit Insurance Corp. and the Office of the Comptroller of the Currency issued the proposal on Tuesday, and the Federal Reserve Board is expected to do so soon.

FDIC Chairman Jelena McWilliams pointed to a rise in both the frequency and severity of cyberattacks, and noted that prompt notification to regulators could help contain the damage.

“The rule proposed by the agencies today provides appropriate balance -- avoiding unnecessarily difficult or time-consuming reporting obligations while ensuring that regulatory agencies are in a position to provide assistance to a bank or the broader financial system when significant computer-security incidents occur,” McWilliams said in a written statement.

Under the proposal, banks would be required to notify their primary federal regulator within 36 hours of making a good-faith determination that an incident could materially disrupt, impair or degrade their operations, or threaten U.S. financial stability. Such a notification could be as simple as making a phone call or sending an email to an agency official.

The proposed rules would also impose new obligations on banks' technology vendors. Once vendors determined that a computer security incident met certain thresholds, they would have to notify their bank customers immediately.

The FDIC said Tuesday that the proposed rule is designed to fill a gap in banks' existing reporting requirements.

Under 15-year-old interagency guidance, banks are supposed to notify their primary regulator "as soon as possible" about incidents involving unauthorized access to sensitive customer information. But that guidance does not apply to disruptive incidents in which no customer data is exposed.

Banks also have obligations to file suspicious activity reports under certain circumstances, but those reports can in some cases be filed as late as 60 days after suspicions are raised.

The proposal released Tuesday cites specific types of incidents that could trigger banks' notification obligations. The list includes large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time, failed system upgrades that result in widespread user outages and ransomware attacks.

"These incidents have the potential to alter, delete or otherwise render a banking organization's data and systems unusable," FDIC staff wrote in a memo to the agency's board. "These incidents can result in customers being unable to access their deposits and other accounts. In rare instances, a significant computer-security incident may jeopardize the viability of a banking organization."

At a congressional hearing in June, a cybersecurity expert said that attacks against the financial sector increased by 238% in the first five months of 2020. "Criminals are increasingly sharing resources and information, and reinvesting their illicit profits into the development of new and even more destructive capabilities," testified Tom Kellermann, head of cybersecurity strategy at VMWare.

Given the rising threat, cybersecurity has been a recent focus of the federal banking agencies. In January, the FDIC and OCC sent a letter to banks that outlined risk-mitigation techniques in the cybersecurity realm, touching on authentication, system configuration, data protection and employee training.

The notice of proposed rulemaking that was issued Tuesday will be open for comment for 90 days from its publication in the Federal Register.

Kevin Wack
Staff Writer, American Banker