VitalLaw™

Banking and Finance Law Daily Wrap Up, BANK SECRECY ACT —Regulators propose 36-hour SAR turnaround for cybersecurity incidents, (Dec. 16, 2020)

Banking and Finance Law Daily Wrap Up

Click to open document in a browser

By Jacob Bielanski

The FDIC, Fed, and OCC jointly estimated the new rule would only produce 150 incidents per year, despite the proposal's expansion of SAR requirements and earlier warnings of an increase in frequency and severity of cyberattacks.

Federal financial regulators have proposed a rule that would require banks to "promptly" file a suspicious activity report (SAR) whenever a computer security incident could "materially disrupt, degrade or impair" operation. According to the December 15 notice, the rule was proposed jointly by the Treasury's Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and the Board of Governors of the Federal Reserve System. Comments on the proposal are due within 90 days from publication of the notice in the *Federal Register*.

A memo from the FDIC regarding the rule noted that regulated financial institutions are already required to submit a SAR to their primary federal regulator for security incidents. However, this requirement only applies to incidents involving sensitive customer data and institutions have up to 60 days to submit the SAR. The FDIC and OCC issued a joint statement on heightened cybersecurity risk in January that noted cyberattacks against banks have increased in frequency and severity in recent years.

"These reports may not be filed with regulatory agencies in time to provide assistance to an affected bank or to coordinate a regulatory or security response to a cyberattack that may affect multiple institutions," FDIC Chairman Jelena McWilliams said in a statement on the rulemaking notice. "The notification requirements included in this proposed rulemaking would address this gap in timely regulatory awareness of the most significant computer-security incidents affecting banking organizations."

The proposed rule would give banks only 36 hours to submit a SAR, as well as expanding the definition beyond merely those involving customer data. Despite this, regulators conservatively estimate among the approximately 5,000 institutions supervised, only about 150 incidents per year would meet the new reporting guidelines. Though the proposal called that number "conservative," it did specifically invite comments on the accuracy of that number.

In addition to the expanded definition and turnaround, the rule would also require bank service providers, as defined in the Bank Service Company Act, to promptly notify banks whenever the service company experiences a similarly defined attack.

Comments on the proposal may be directed through any of the three federal regulators.

RegulatoryActivity: BankingFinance BankingOperations BankSecrecyAct CyberPrivacyFeed DataBreach FederalReserveSystem FedTracker FinancialStability FinTech GCNNews Privacy