Final Rule on Computer-Security Incident Notification

Last Updated: November 18, 2021

Technological advancement in banking has lowered the cost of financial services and products, expanded the pool of creditworthy consumers, and increased access to financial services. As the nation's deposit insurer and primary supervisor of community banks, the FDIC is also cognizant of the critical role of innovation in allowing community banks to remain competitive in the modern world. At the same time, however, as technology has evolved, so have the cybersecurity risks with which banks must grapple. In recent years, the frequency and severity of cyberattacks against financial institutions have increased.[1]

The final rule the FDIC has approved, along with the Office of the Comptroller of the Currency (OCC) and the Board of Governors of the Federal Reserve System (Board), addresses a gap in timely notification to the banking agencies of the most significant computer-security incidents affecting banking organizations, allowing the FDIC and our fellow banking supervisors to be better positioned to understand and to respond to cybersecurity threats across the banking sector.

The final rule requires a bank to notify its primary federal regulator of a computer-security incident that rises to the level of a "notification incident," namely a computer-security incident that has materially disrupted or degraded – or is reasonably likely to materially disrupt or degrade – the viability of a bank's operations, its ability to deliver banking products and services, or the stability of the U.S. financial sector. The agencies made several changes to the proposed rule to address concerns about over-reporting of incidents, including narrowing the scope of the definitions of "computer-security incident" and "notification incident."

The final rule also requires a bank's service provider to notify its client bank if such service provider experiences a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, banking services for four or more hours.

The final rule seeks to allow the banking supervisors to be informed of the most significant cyberattacks in a timely fashion while avoiding unnecessarily difficult or time-consuming reporting obligations. The final rule therefore does not require an assessment of the incident to fulfill the notification requirement.

The final rule has been developed jointly with the Board and the OCC, and I commend the efforts of our staffs in this thoughtful and balanced interagency effort.

---

[1] *See* FDIC, FIL-03-2020, Heightened Cybersecurity Risk Considerations (Jan. 16, 2020), available at https://www.fdic.gov/news/financial-institution-letters/2020/fil20003.html.