Financial Institution Letter

Computer-Security Incident Notification Final Rule

November 18, 2021 | FIL-74-2021

Summary:

The Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Board), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) have issued a joint final rule to establish computer-security incident notification requirements for banking organizations and their bank service providers.

The rule will provide the agencies with early awareness of emerging threats to banking organizations and the broader financial system, including potentially systemic cyber events.

A copy of the Final Rule can be found on the FDIC's website.

Statement of Applicability: This Financial Institution Letter (FIL) applies to all FDIC-supervised institutions.

Highlights:

- FDIC-supervised banking organizations will be required to notify the FDIC as soon as possible and no later than 36 hours after the banking organization determines that a computer-security incident that rises to the level of a notification incident has occurred. The banking organization must provide this notification to the appropriate FDIC supervisory office, or an FDIC-designated point of contact, through email, telephone, or other similar methods that the FDIC may prescribe.

- The rule defines computer-security incident as an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits.

- A notification incident is defined as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's: (i) ability 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) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) operations, 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. For example, a notification incident may include a major computer-system failure; a cyber-related interruption, such as a distributed denial of service or ransomware attack; or another type of significant operational interruption.

- The rule also requires a bank service provider to notify at least one bank-designated point of contact at each affected customer banking organization as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to disrupt or degrade, covered services provided to the banking organization for four or more hours. If the banking organization has not previously provided a designated point of contact, the notification must be made to the banking organization's chief executive officer and chief information officer or to two individuals of comparable responsibilities.

- The final rule takes effect on April 1, 2022, with full compliance extended to May 1, 2022. The FDIC will provide supervised institutions logistics for FDIC notification in early 2022.

Attachment:

Final Rule

Distribution:

FDIC-Supervised Institutions

Suggested Routing:

Chief Information Officer
Chief Information Security Officer
Chief Operating Officer
Chief Risk Officer
Chief Technology Officer