THOMPSON COBURN LLP

insights

TYPES NOT MAPPED YET December 16, 2021 | TTR not mapped yet | Luke Sosnicki, Elizabeth (Libby) A. James

Computer-security incident notification requirement takes effect April 1, 2022

The Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency (the "prudential banking regulators") issued a final rule regarding the Computer-Security Incident Notification Requirement.

The final rule requires that a "banking organization" notify its primary federal regulator of a "computer-security incident" that meets the level of a "notification incident." The notification must be given to the primary federal regulator as soon as possible, and no later than 36 hours after its determined that a notification incident has happened. The final rule also contains a requirement that a "bank service provider," defined as a "bank service company or other person that performs [services covered under the Bank Service Company Act]," notify a 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 materially disrupt or degrade, covered services provided to such banking organization for four or more hours."

The rule defines a "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." 12 C.F.R. §§ 53.2(4), 225.301(4), 304.22(4). A "Notification incident is 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." 12 C.F.R. §§ 53.2(7), 225.301(7), 304.22(7).

The new incident reporting requirements are separate from existing breach notification requirements issued in 2005 under the safeguarding authority granted to the prudential banking regulators by the Gramm-Leach-Bliley Act. The rule takes effect on April 1, 2022, and the compliance date is May 1, 2022.

authorsTest

luke

Luke Sosnicki

elizabeth

Elizabeth (Libby) A. James