KPMG

Regulatory Alert

Regulatory Insights

November 2021

Cyber incident notifications

The Administration has called for improvements to national cybersecurity defenses in response to "persistent and increasingly sophisticated cyber campaigns." The federal banking agencies note that cyberattacks targeting the financial services industry are both more frequent and severe, raising the importance of early warnings about potential threats to the banking sector and financial stability more broadly. The 36-hour notification requirement is much shorter than the 72-hour notices required by either the NY DFS Cybersecurity Rule or the EU's GDPR, though the notice may be completed simply via email or phone.

The Federal Reserve, OCC, and FDIC issued a final rule that establishes two primary requirements concerning "computer-security incidents." In particular:

- A supervised banking organization under the authority of the agencies must:
  - Notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident" (as defined in the rule.)
  - Provide notification as soon as possible, but within 36 hours of determining that the incident has occurred. The notification is intended to serve as an "early alert" and may be provided via email or telephone or similar method.
- A "bank service provider" must notify its banking organization customers as soon as possible when the 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, the covered services provided to the banking organization customer for four or more hours.

Compliance with the final rule is required for all supervised banking organizations by May 1, 2022.

Key definitions:

- ***Computer-security incident:*** 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. This definition is intended to be consistent with the definition from the National Institute of Standards and Technology (NIST). Computer-security incidents may include major computer-system failures; cyber-related interruptions, such as distributed denial of service and ransomware attacks; or other types of significant operational interruptions.
- ***Notification incident:*** A computer-security incident that a bank believes in good faith could materially disrupt, degrade, or impair:
  - The ability of the bank to carry out operations, activities, or processes, or delivery of banking products and services to a material portion of its customer base
  - Any business line of a bank, including associated operations, services, functions, and support, and would result in a material loss of revenue, profit, or franchise value

  - Those operations of a bank, 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.
- ***Bank service provider:*** A bank service company or other person who performs "covered services" (subject to the Bank Service Company Act (BSCA)), except for a designated financial market utility (FMU).

For additional information please contact Amy Matsuo, Matt Miller, or Orson Lucas.

Contact the author:

Amy Matsuo
Principal and Leader
ESG and Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia