What: New cybersecurity reporting requirements for banks

The Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) approved a final rule that places reporting requirements on banks and bank service providers. Under this new rule, banks must notify their primary federal regulator of any computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a bank’s ability to carry out banking operations or deliver banking products and services.

When: May 1, 2022

What: Definition of computer-security incident

- A computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a bank’s ability to carry out banking operations or deliver banking products and services.

Preparation:

- Develop a workflow to trigger for major events in the incident response cycle.
- Designate a team to take primary responsibility for incident reporting.
- Establish a reporting channel with all primary examiners and regulatory contacts.
- Prepare incident reporting forms for all major events in the incident response cycle.
- Update your incident response plan to include these new reporting requirements.
- Allow the bank to practice meeting these deadlines during tabletop exercises.

FAQ:

- What must banks do?
  - Must notify affected bank customers as soon as possible of any computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.
  - Must notify primary federal regulator of any computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a bank’s ability to carry out banking operations or deliver banking products and services.

- What's the compliance date?
  - The final rule applies to the following banking organizations: national banks, Federal savings and loan associations, and Federal branches and agencies of foreign banks; includes all U.S. bank holding companies and savings and loan holding companies; includes all insured state member banks; the U.S. operations of foreign banking organizations; and insured State branches, branches and agencies of foreign banks.

- Who is impacted?
  - For the FDIC, “banking organizations” includes all insured state nonmember savings associations, and Federal branches and agencies of foreign banks.
  - For the OCC, “banking organizations” includes all insured state nonmember savings associations, and Federal branches and agencies of foreign banks.
  - For the Board, “banking organizations” includes all insured state nonmember savings associations, and Federal branches and agencies of foreign banks.

- What is required of bank service providers?
  - Must notify primary federal regulator of any computer-security incident.
  - Must notify affected bank customers as soon as possible of any computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

- What is considered a notification incident?
  - A large scale distributed denial of service (DDoS) attack.
  - A computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a bank’s ability to carry out banking operations or deliver banking products and services.

- What is required of banks?
  - Must notify affected bank customers as soon as possible of any computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

- What's required of bank service providers?
  - Must notify primary federal regulator of any computer-security incident.
  - Must notify affected bank customers as soon as possible of any computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.
  - Must notify bank service provider of any computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a bank’s ability to carry out banking operations or deliver banking products and services.

- What is the new data breach notification rule?
  - A large scale distributed denial of service (DDoS) attack.

- What's the new data breach notification rule?
  - A large scale distributed denial of service (DDoS) attack.

- What's the impact on banks?
  - A large scale distributed denial of service (DDoS) attack.

- What impact will the new rule have on banks?
  - A large scale distributed denial of service (DDoS) attack.

- What impact will the new rule have on banks?
  - A large scale distributed denial of service (DDoS) attack.

- What impact will the new rule have on banks?
  - A large scale distributed denial of service (DDoS) attack.