AT&T Business

New **cybersecurity** reporting requirements for banks

What:

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 banking service providers. Under this new rule, banks must report any "computer security incident" that rises to the level of a "notification incident" within 36 hours to its primary federal regulators.

Federal Registry Details on NEW Incident Notification Requirements:
Federal Register :: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

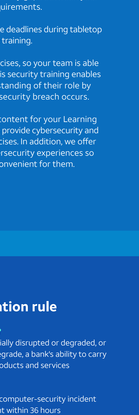
When:

This rule goes into effect on April 1, 2022, and banks are required to comply by May 1, 2022.

Who:

The final rule applies to the following banking organizations:

- For the OCC, "banking organizations" includes national banks, Federal savings associations, and Federal branches and agencies of foreign banks.
- For the Board, "banking organizations" includes all U.S. bank holding companies and savings and loan holding companies; state member banks; the U.S. operations of foreign banking organizations; and Edge and agreement corporations.
- For the FDIC, "banking organizations" includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations.
- Bank service providers.



Preparation:

- Determine who will be responsible for reporting incidents to the regulators and customers.
- Update your incident response plan to include these new reporting requirements and deadlines.
  - It's essential to fit those requirements into your current incident response plan.
    - AT&T Consulting for Incident Response & Forensics offers an in-depth look at your Incident Response Plan (IRP) and will identify gaps between your IRP and the new reporting requirement.
    - AT&T Consulting also offers threat capability assessments and security maturity assessments to identify gaps between your readiness and the new reporting requirements.
  - Allow the bank to practice meeting these deadlines during tabletop exercises and internal incident response training.
    - AT&T Consulting offers tabletop exercises, so your team is able to respond to incidents efficiently. This security training enables each person to develop a full understanding of their role by simulating a response when a cybersecurity breach occurs.
    - AT&T Consulting will create custom content for your Learning Management System (LMS), as well as provide cybersecurity and capability development training exercises. In addition, we offer on-demand (simulation-based), cybersecurity experiences so your team can learn when it's most convenient for them.

FAQ:

New data breach notification rule

What is considered a notification 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

What's required of banks?
Must notify primary federal regulator of any computer-security incident that rises to the level of a notification incident within 36 hours

What's required of bank service providers?
Must notify affected bank customers as soon as possible of computer-security incidents that have caused, or are reasonably likely to cause, a material service disruption or degradation for four or more hours

What's the compliance date?
May 1, 2022

Example scenario:

A large scale distributed denial of service (DDoS) attack

A large scale distributed denial of service attack that disrupts customer account access for an extended period of time (e.g., more than 4 hours) could be considered a notification incident that triggers reporting requirements. Therefore, it's essential to speak with someone that who can walk you through the practical applications of this rule.

- AT&T Consulting could be engaged to review your current cybersecurity policies and procedures to identify deficiencies with compliance to the new reporting rules.

To learn more about how AT&T Cybersecurity consulting can help your business meet these new requirements, contact your AT&T Business representative.

Definition of computer-security incident

- Results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or
- Constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.