RESCINDED

OCC Bulletin 2021-3 | January 14, 2021

Transmittal rescinded.

Computer-Security Incident Notification: Notice of Proposed Rulemaking

To

Chief Executive Officers of All National Banks, Federal Savings Associations, and Federal Branches and Agencies; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Summary

On January 12, 2021, the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation published a notice of proposed rulemaking (NPR) that would require a covered entity to provide its primary federal regulator with prompt notification of any "computer-security incident" that rises to the level of a "notification incident," as defined in the NPR. The deadline for comments on the proposed rule is April 12, 2021.

Note for Community Banks

The proposed rule would apply to community banks.[1]

Highlights

- The proposed rule would require banks to notify the OCC as soon as possible and no later than 36 hours after the bank believes in good faith that a "notification incident" has occurred. The notification may be provided in any form of written or oral communication, including through any technological means, to the OCC's designated point of contact.
- The proposed rule would also require a bank service provider to notify at least two individuals at each affected bank customer immediately after it experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided subject to the Bank Service Company Act for four or more hours.

Background

Internet crime and cyberattacks reported to federal law enforcement have increased in frequency and severity in recent years. These types of attacks may use destructive malware or other cybersecurity exploits to target weaknesses in a bank's computers or networks. Some exploits have the potential to alter, delete, or otherwise render a bank's data and systems unusable. Depending on the scope of the incident, a bank's data and system backups may also be affected, which can severely affect its ability to recover operations. In addition, banks have

become increasingly reliant on bank service providers to provide essential, technology-related products and services. These services are also vulnerable to cyber threats.

The proposed rule would ensure that the OCC knows about and can respond to significant computer-security incidents at banks.

Further Information

Please contact Patrick Kelly, Director, Critical Infrastructure Policy, (202) 649-5519; or Jennifer Slagle Peck, Counsel, or Priscilla Benner, Senior Attorney, Chief Counsel's Office, (202) 649-5490.

Bao Nguyen
Principal Deputy Chief Counsel

Related Link

- "Computer-Security Incident Notification Requirements for Banking Organizations and their Bank Service Providers: Proposed Rule" (PDF)

---

[1] "Banks" refers to national banks, federal savings associations, and federal branches and agencies of foreign banking organizations.

Topic(s): ■ BANK INFORMATION TECHNOLOGY (BIT) ■ OCC REGULATIONS