

UPDATES

U.S. Federal Bank Regulators Require Notifications For Material Cybersecurity Incidents

November 23, 2021

On November 18, 2021, a group of federal bank regulators announced [a final rule](#) requiring banks to notify their primary federal regulator of any “significant computer-security incidents.” Regulators must be notified no later than 36 hours after the bank has determined that the incident triggers the rule’s notification requirement. Further, bank service providers are now required to promptly notify all affected banks whenever a cybersecurity disruption lasts for four or more hours.

The rule is the latest regulation requiring entities that have suffered a cybersecurity incident to promptly notify a government agency. Unlike some of those regulations, this rule is not linked to compromised consumer data.

Background

The rule was initially proposed in January 2021. In the intervening months, both President Joe Biden and Federal Reserve Chair Jerome Powell have described cyberattacks as a major threat to the private and public sectors. In May 2021, President Biden issued an executive order to bolster federal cybersecurity standards. Congress, as part of its annual defense policy bill, is debating a proposal to require certain entities to report cyberintrusions to the federal government.

The rule was jointly issued by the Board of Governors of the Federal Reserve (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC). All three have adopted nearly identical versions of the rule, differing only to identify the specific banking organizations subject to their individual authority. Each regulator cites different statutes as the basis of its authority, including the Federal Deposit Insurance Act, the Home Owners’ Loan Act, the Bank Service Company Act, and the Federal Reserve Act. The Gramm-Leach-Bliley Act is not a basis of the rule’s authority.

The agencies note the increasing frequency and severity of cyberattacks on the financial services industry as a key motivator for the rule. They write that the new rule will allow them to better detect and assess cybersecurity threats, facilitate assistance to victims, and provide information to other banks.

The rule has two prongs: (1) Banks are now required to notify their primary federal regulator when they suffer from certain disruptive cybersecurity incidents, and (2) bank service providers must notify affected

customer banks when an incident disrupts covered services for four or more hours.

Banks Must Notify Their Primary Federal Regulator

Each regulator defines a banking organization according to its jurisdiction.

- For the OCC, this includes national banks, federal savings associations, and federal branches of foreign banks.
- The Board subjects all U.S. bank holding companies, state member banks, and U.S. operations of foreign banks to the regulation.
- The FDIC defines “banking organizations” to include all insured state nonmember banks and insured state-licensed branches of foreign banks.

The rule does not apply to financial market utilities, financial technology firms, and nonbank OCC-chartered entities. Altogether, the regulation will apply to most traditional depository institutions.

The rule is concerned about actual harm to the confidentiality, integrity, or availability of an information system — or the information on the system. These occurrences are “computer-security incidents.”

When a “computer-security incident” materially disrupts a bank’s ability to carry out ordinary operations, results in a material loss in revenue, or poses a threat to the financial stability of the United States, the bank must notify its primary federal regulator. These kinds of computer-security incidents are referred to as “notification incidents.”

The rule provides a nonexhaustive list of “notification incidents” that would require notification:

- large-scale distributed denial of service attacks disrupting customer access for more than four hours
- a bank service provider experiencing widespread system outages with no determinable recovery time
- a failed system upgrade resulting in widespread user outages
- an unrecoverable system failure triggering the bank’s disaster recovery plan
- a computer hacking incident disabling banking operations for an extended period of time
- malware on a bank’s network presenting an imminent threat to core business lines or operations
- a ransom malware attack encrypting a core banking system or backup data

Once a bank determines that a notification incident has occurred, it must alert its primary federal regulator promptly and no later than 36 hours after the determination was made.

Bank Service Providers Must Notify Banks

The second prong of the rule requires bank service providers to notify banks affected by a disruption as soon as possible. A bank service provider is a “bank service company” or a person that performs services subject to the Bank Service Company Act, except for financial market utilities.

Once a service provider has determined that a “computer-security incident” is likely to materially disrupt or degrade covered services for four or more hours, it must notify affected banks as soon as possible. This requirement is independent of any existing contractual provisions. The rule does not apply to scheduled maintenance or tests. Bank service providers do not have to determine whether the incident is a “notification incident.”

After receiving a notification from the provider, a bank must determine whether the incident is a “notification incident.” If it is, the bank has 36 hours to notify the regulator. The agencies have stated that they will not penalize a bank because the service provider fails to comply with the notification requirement.

Next Steps

The rule is effective April 1, 2022; entities must be compliant by May 1, 2022.

Banks will want to revise their internal policies to ensure they are promptly identifying and assessing cyberincidents. Additionally, banks and bank service providers will want to assess whether any existing notification processes are designed to ensure that the banks are receiving timely notice.

All banking entities subject to the jurisdiction of the Board, FDIC, or OCC should promptly review the rule to ensure they are compliant by May 1.

Thank you to Sidley Law Clerk Vishnu Tirumala for his significant contribution to this Update

CONTACTS

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

David E. Teitelbaum , Partner	+1 202 736 8683, dteitelbaum@sidley.com
Colleen Theresa Brown , Partner	+1 202 736 8465, ctbrown@sidley.com
Michael D. Lewis , Partner	+1 202 736 8959, michael.lewis@sidley.com
Vishnu Tirumala , Managing Associate	+1 202 736 8147, vtirumala@sidley.com

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices.

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

© Sidley Austin LLP