Morgan Lewis

BITE-SIZED BANKING BULLETIN

FEDERAL BANKING REGULATORS ISSUE 36-HOUR CYBERSECURITY BREACH NOTIFICATION REQUIREMENT

Federal Banking Regulators Issue 36-Hour Cybersecurity Breach Notification Requirement

Beth Herrington
Alex Berger

February 7, 2022

Presenters

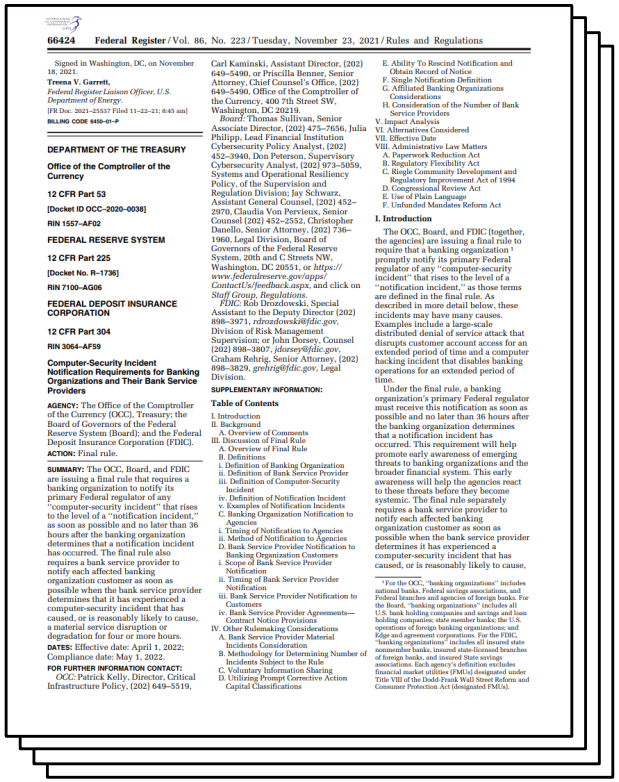
Beth Herrington
Partner | Chicago

Alex Berger
Associate | Chicago

Morgan Lewis

What is this New Rule Issued By Regulators?

- "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers"
- Three US Agencies: Office of the Comptroller of the Currency (OCC); Federal Reserve Board (FRB) and Federal Deposit Insurance Corporation (FDIC)
- Issued November 18, 2021
- Effective April 1, 2022
- **Full compliance by May 1, 2022**



66424 Federal Register / Vol. 86, No. 223 / Tuesday, November 23, 2021 / Rules and Regulations

Signed in Washington, DC, on November 18, 2021.

Treena V. Garrett,

Federal Register Liaison Officer, U.S. Department of Energy.

[FR Doc. 2021–25537 Filed 11–22–21; 8:45 am]

BILLING CODE 6450–01–P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 53

[Docket ID OCC–2020–0038]

RIN 1557–AF02

FEDERAL RESERVE SYSTEM

12 CFR Part 225

[Docket No. R–1736]

RIN 7100–AG06

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Part 304

RIN 3064–AF59

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

AGENCY: The Office of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC).

ACTION: Final rule.

SUMMARY: The OCC, Board, and FDIC are issuing a final rule that requires a banking organization to notify its primary Federal regulator of any ''computer-security incident'' that rises to the level of a ''notification incident,'' as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

DATES: Effective date: April 1, 2022; Compliance date: May 1, 2022.

FOR FURTHER INFORMATION CONTACT:

OCC: Patrick Kelly, Director, Critical Infrastructure Policy, (202) 649–5519, Carl Kaminski, Assistant Director, (202) 649–5490, or Priscilla Benner, Senior Attorney, Chief Counsel's Office, (202) 649–5490, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219.

Board: Thomas Sullivan, Senior Associate Director, (202) 475–7656, Julia Philipp, Lead Financial Institution Cybersecurity Policy Analyst, (202) 452–3940, Dan Peterson, Supervisory Cybersecurity Analyst, (202) 973–5059, Systems and Operational Resiliency Policy, of the Supervision and Regulation Division; Jay Schwarz, Assistant General Counsel, (202) 452–2970, Claudia Von Pervieux, Senior Counsel (202) 452–2552, Christopher Danello, Senior Attorney, (202) 736–1960, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551, or *https://www.federalreserve.gov/apps/ContactUs/feedback.aspx*, and click on *Staff Group, Regulations.*

FDIC: Rob Drozdowski, Special Assistant to the Deputy Director (202) 898–3971, *rdrozdowski@fdic.gov*, Division of Risk Management Supervision; or John Dorsey, Counsel (202) 898–3807, *jdorsey@fdic.gov*, Graham Rehrig, Senior Attorney, (202) 898–3829, *grehrig@fdic.gov*, Legal Division.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction

The OCC, Board, and FDIC (together, the agencies) are issuing a final rule to require that a banking organization [1] promptly notify its primary Federal regulator of any ''computer-security incident'' that rises to the level of a ''notification incident,'' as those terms are defined in the final rule. As described in more detail below, these incidents may have many causes. Examples include a large-scale distributed denial of service attack that disrupts customer account access for an extended period of time and a computer hacking incident that disables banking operations for an extended period of time.

Under the final rule, a banking organization's primary Federal regulator must receive this notification as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. This requirement will help promote early awareness of emerging threats to banking organizations and the broader financial system. This early awareness will help the agencies react to these threats before they become systemic. The final rule separately requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines it has experienced a computer-security incident that has caused, or is reasonably likely to cause,

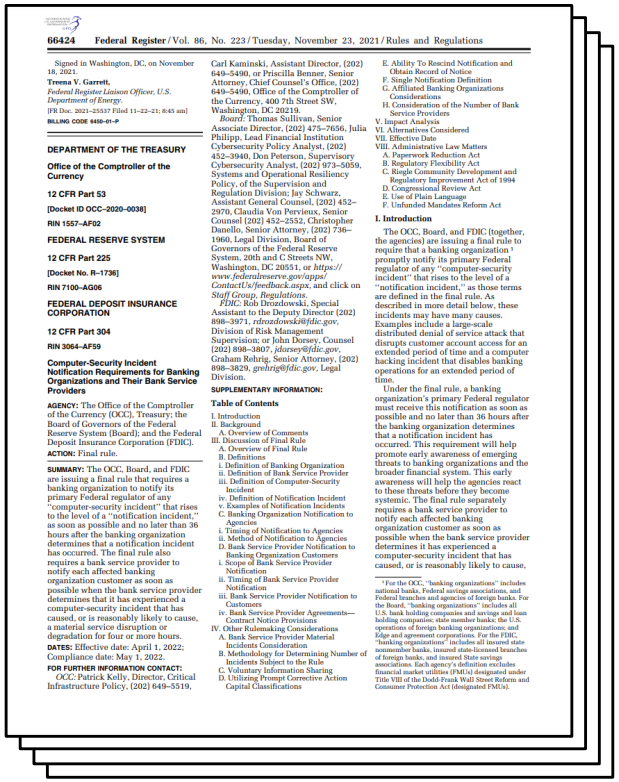
[1] For the OCC, ''banking organizations'' includes national banks, Federal savings associations, and Federal branches and agencies of foreign banks. For the Board, ''banking organizations'' includes all U.S. bank holding companies and savings and loan holding companies; state member banks; the U.S. 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. Each agency's definition excludes financial market utilities (FMUs) designated under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (designated FMUs).

Morgan Lewis

What is this New Rule Issued By Regulators?

- Requires banking organization to notify its primary Federal regulator of "computer-security incident" rising to level of "notification incident," as soon as possible and *no later than 36 hours* after banking organization determines notification incident has occurred.

- Requires bank service provider to notify each affected banking organization customer as soon as possible when bank service provider determines it has experienced computer-security incident that caused, or is reasonably likely to cause, material service disruption or degradation for 4 or more hours.



66424 Federal Register / Vol. 86, No. 223 / Tuesday, November 23, 2021 / Rules and Regulations

Signed in Washington, DC, on November 18, 2021.

Treena V. Garrett,

Federal Register Liaison Officer, U.S. Department of Energy.

[FR Doc. 2021–25537 Filed 11–22–21; 8:45 am]

BILLING CODE 6450–01–P

DEPARTMENT OF THE TREASURY

Office of the Comptroller of the Currency

12 CFR Part 53

[Docket ID OCC–2020–0038]

RIN 1557–AF02

FEDERAL RESERVE SYSTEM

12 CFR Part 225

[Docket No. R–1736]

RIN 7100–AG06

FEDERAL DEPOSIT INSURANCE CORPORATION

12 CFR Part 304

RIN 3064–AF59

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

AGENCY: The Office of the Comptroller of the Currency (OCC), Treasury; the Board of Governors of the Federal Reserve System (Board); and the Federal Deposit Insurance Corporation (FDIC).

ACTION: Final rule.

SUMMARY: The OCC, Board, and FDIC are issuing a final rule that requires a banking organization to notify its primary Federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. The final rule also requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines that it has experienced a computer-security incident that has caused, or is reasonably likely to cause, a material service disruption or degradation for four or more hours.

DATES: Effective date: April 1, 2022; Compliance date: May 1, 2022.

FOR FURTHER INFORMATION CONTACT:

OCC: Patrick Kelly, Director, Critical Infrastructure Policy, (202) 649–5519, Carl Kaminski, Assistant Director, (202) 649–5490, or Priscilla Benner, Senior Attorney, Chief Counsel's Office, (202) 649–5490, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219.

Board: Thomas Sullivan, Senior Associate Director, (202) 475–7656, Julia Philipp, Lead Financial Institution Cybersecurity Policy Analyst, (202) 452–3940, Don Peterson, Supervisory Cybersecurity Analyst, (202) 973–5059, Systems and Operational Resiliency Policy, of the Supervision and Regulation Division; Jay Schwarz, Assistant General Counsel, (202) 452–2970, Claudia Von Pervieux, Senior Counsel (202) 452–2552, Christopher Danello, Senior Attorney, (202) 736–1960, Legal Division, Board of Governors of the Federal Reserve System, 20th and C Streets NW, Washington, DC 20551, or *https://www.federalreserve.gov/apps/ContactUs/feedback.aspx*, and click on *Staff Group, Regulations.*

FDIC: Rob Drozdowski, Special Assistant to the Deputy Director (202) 898–3971, *rdrozdowski@fdic.gov*, Division of Risk Management Supervision; or John Dorsey, Counsel (202) 898–3807, *jdorsey@fdic.gov*, Graham Rehrig, Senior Attorney, (202) 898–3829, *grehrig@fdic.gov*, Legal Division.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. Introduction

The OCC, Board, and FDIC (together, the agencies) are issuing a final rule to require that a banking organization [1] promptly notify its primary Federal regulator of any "computer-security incident" that rises to the level of a "notification incident," as those terms are defined in the final rule. As described in more detail below, these incidents may have many causes. Examples include a large-scale distributed denial of service attack that disrupts customer account access for an extended period of time and a computer hacking incident that disables banking operations for an extended period of time.

Under the final rule, a banking organization's primary Federal regulator must receive this notification as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. This requirement will help promote early awareness of emerging threats to banking organizations and the broader financial system. This early awareness will help the agencies react to these threats before they become systemic. The final rule separately requires a bank service provider to notify each affected banking organization customer as soon as possible when the bank service provider determines it has experienced a computer-security incident that has caused, or is reasonably likely to cause,

[1] 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. Each agency's definition excludes financial market utilities (FMUs) designated under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (designated FMUs).

Which Organizations Must Comply with the Rule?

"Banking Organizations"

OCC: includes national banks, federal savings associations, and federal branches and agencies of foreign banks.

FRB: includes all US bank holding companies and savings and loan holding companies; state member banks; the US operations of foreign banking organizations; Edge and agreement corporations.

FDIC: includes all insured state nonmember banks, insured state-licensed branches of foreign banks and state savings associations.

Which Organizations Must Comply with the Rule?

"Bank Service Providers"

- "Bank service company" or other person who performs "covered services."

- "Covered services:" services performed by "person" subject to Bank Service Company Act.

How Does the Rule Affect Banking Organizations?

- Banking organization must notify primary regulator ***as soon as possible*** and ***no later than 36 hours after*** it determines that a "computer-security incident" occurred that rises to the level of a "notification incident."

  – Clock does not begin until thresholds in each definition satisfied.

  – Banking organizations may take position that time investigating incident does not count against clock until conditions are met.

What are "Computer-Security Incidents" Under the Rule?

- Occurrences that results in ***actual harm*** to confidentiality, integrity, or availability of information system or information that system processes, stores, or transmits.
  - No definition of "actual harm."
  - Looking at other laws, fairly high standard.

What are "Notification Incidents" Under the Rule?

- Incident must have materially disrupted or degraded or is reasonably likely to materially disrupt or degrade banking organization's:
  - Ability to carry out banking operations, activities or processes
  - Business lines
  - Operations

How is this Rule Different than Traditional Breach Notification Laws?

- This Rule focuses on operational impacts of security incident.

- In addition to "actual harm" threshold, notifications aren't triggered until "material disruption" or "degradation standard" met.
  - Some affected banks may reasonably conclude no reporting obligations.

- All Three Federal Agencies recognize this.

How Does the Rule Affect Bank Service Providers?

- BSPs must notify "bank-designated point of contact" at each banking organization affected by computer-security incident ***as soon as possible*** after determining that it has experienced computer security incident that:

  – "has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to such banking organization for four or more hours."

Important Differences Associated with Bank Service Providers' Obligations

1. Establishing a bank-designated point of contact

2. Tripper trigger

3. Routine maintenance exception

What Actions to Take Next?

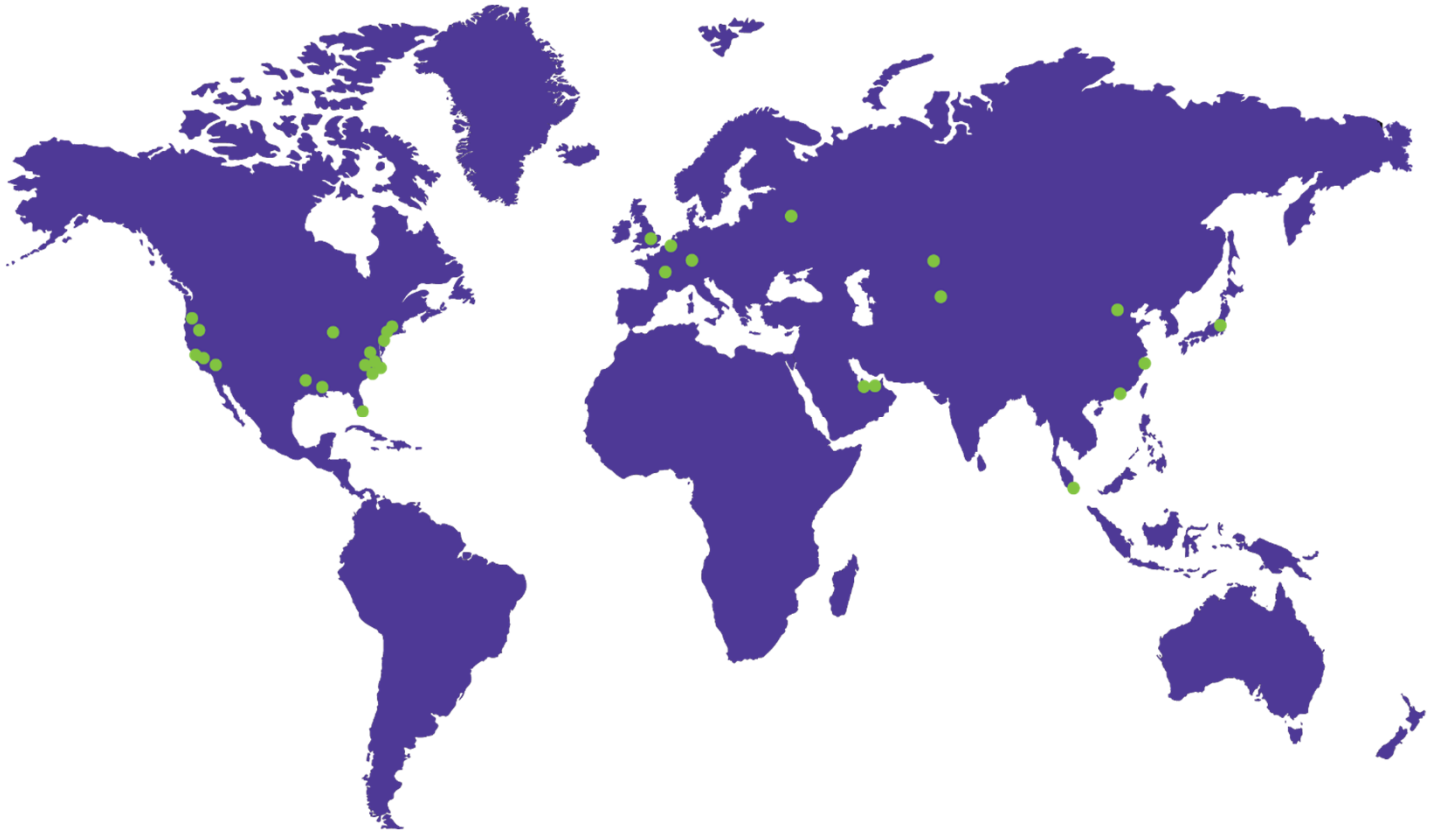
- Look for regulators' specific guidance on logistics to report incidents.
- Review and update existing incident response plans to ensure that notification incidents are properly escalated and addressed.
- Review and update agreements with service providers so there are explicit contractual obligations to comply with requirements under Rule.
- Be in compliance by May 1, 2022

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU