Cybersecurity

IT Incident Response and Reporting

Federal Reserve Bank of Dallas

Given the heightened cyber threat environment, as your primary regulator, we would like to remind you of our expectations for effective computer security incident response and reporting. As of May 1, 2022, supervisory expectations increased as a result of a final rule issued by federal banking regulators.

How do I proceed?

Existing SR 05-23 expectations to report loss of "sensitive" customer data remain in effect. "Sensitive" customer information includes name, address, or telephone number **and** one of the following:

- Social security number
- Driver's license number
- Account number
- Credit or debit card number
- Personal identification number (PIN) or password

When is SR 22-4 computer-security incident reporting to the Federal Reserve required?

- A banking organization[1] must notify the Federal Reserve about a notification incident as soon as possible and **no later than 36 hours** after the firm determines an incident has occurred.
- A notification incident is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's
  - Ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base;
  - Business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or
  - Operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

---

[1] A banking organization 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. Banking organizations should report covered incidents to the Federal Reserve that occur at non-bank subs that are not otherwise consolidated in a banking charter but may have broader implications for the whole organization. Similarly banking organizations should report covered incidents that occur at the parent organization.

Note that a notification incident could include an operational failure or IT error that does not result from a malicious breach of a banking organization's IT systems.

Collaborate with Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Department

- Provide your BSA/AML staff with relevant and available incident details, such as the Internet Protocol address with timestamps, virtual-wallet information, and device identifiers.

How do I report?

For Incidents reportable under both SR 22-4 and SR 05-23, reporting using the SR 22-4 process will also fulfill SR 05-23 requirements.

For SR 22-4 - Computer-Security Incidents:

- Email the Federal Reserve System incident mailbox at incident@frb.gov and notify your Central Point of Contact, or
- Contact the Incident Notification Line at 866-364-0096

For SR 05-23–Sensitive Customer Data Incidents:

- Email the Dallas BS&R Incident mailbox:
  - BSR.Incident.Report@dal.frb.org
- Contact an IT Director of Examinations:
  - Jason Anthony, jason.anthony@dal.frb.org / 214.922.6982
  - Drew Wilson, drew.wilson@dal.frb.org / 214.922.6252

For more information

- Visit www.dallasfed.org/banking/IT for more information on cybersecurity risk management resources and IT regulatory requirements.
- SR 05-23—Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- SR 22-4—Contact Information in Relation to Computer Security Incident Notification Requirements
- Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers. 12 CFR Part 225 [Docket No. R-1736] RIN 7100-AG06
- FinCEN FIN-2021-A004 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments
- Office of Foreign Assets Control Updated Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments
- FinCEN FIN-2020-A005 Advisory on Cybercrime and Cyber-Enabled Crime exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic
- FinCEN FIN-2016-A005 Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime
- FinCEN FIN-2022-FCT1 Fact Sheet on the Rapid Response Program (RRP)