Overview

Cybersecurity Incident Notification Rules for Financial Institutions

Dan Pepper and Esther Clovis, Norton Rose Fulbright US LLP

Bloomberg Law

Cybersecurity Incident Notification Rules for Financial Institutions

Contributed by Dan Pepper and Esther Clovis, Norton Rose Fulbright US LLP

Financial institutions that experience cybersecurity incidents may be subject to various reporting requirements. It is important to note that some may be subject to multiple regulations with different timing requirements. Further, entities should evaluate each cybersecurity incident on a case-by-case basis to determine whether or not the incident rises to the level of triggering notification requirements.

The Joint Computer-Security Incident Notification Rule

The joint Computer-Security Incident Notification Rule, issued jointly by the Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), and Federal Deposit Insurance Corporation (FDIC), requires banking organizations to notify federal regulators of any "computer-security incident" within 36 hours of determining that the incident occurred, if the incident rises to the level of a "notification incident". Computer-Security Incident Notification Requirement for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021).

A **computer-security incident** is "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits." 86 Fed. Reg. 66,424 (Nov. 23, 2021). However, not all computer-security incidents" trigger the notification requirement.

A **notification incident** is defined as "a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's 1) ability to carry out banking operations, activities or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business, 2) business line(s), including associated operation, services, functions and support, that upon failure would result in a material loss of revenue, profit or franchise value, or 3) 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." 86 Fed. Reg. 66,424 (Nov. 23, 2021).

Financial entities subject to the joint Computer-Security Incident Notification rule must also notify customers of any computer-security incident that will materially and negatively impact or interfere with customers' covered service for four hours or more. 86 Fed. Reg. 66,424 (Nov. 23, 2021).

Safeguards Rule

Financial institutions subject to their applicable federal regulator's Safeguards Rule that experience computer-security incidents are also subject to the notification requirements of the Safeguards Rule—such entities are required to notify their primary federal regulator as soon as possible when an unauthorized user accesses a customer's sensitive information. 12 C.F.R.pt. 30, app'x B, supp. A (OCC); 12 C.F.R.part 208, app'x D-2 (FRB); 12 C.F.R.part 225, app'x F (FRB); 12 C.F.R.part 364, app'x B (FDIC). This means that some institutions may be subject to multiple notification requirements. *See* Comparison Table – GLBA Privacy & Data Security: Federal & State Regulatory Authority.

Other Agencies

- **NYDFS**: Financial institutions subject to the New York Department of Financial Services (NYDFS) Cybersecurity Regulations must notify the NYDFS within 72 hours of a cybersecurity event. 23 NYCRR § 500.17. *See* Overview - New York Department of Financial Services (NYDFS) Cybersecurity Requirements.
- **SEC**: Public companies regulated by the Securities and Exchange Commission (SEC) must report material cybersecurity incidents, and covered entities must also disclose such events and risks. Systems Compliance and Integrity entities must also report any "SCI events." SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018); 17 C.F.R.§ 242.1002.
- **CFTC**: Derivative clearing organizations subject to the Commodity Futures Trading Commission (CFTC) must report "exceptional" cybersecurity events. 17 C.F.R.§§ 15.00, 39.18(g).

