
Federal Financial Regulators Propose Requiring Banks Report Cyber Incidents Within 36 Hours

DECEMBER 22, 2020

On December 17, 2020, the Office of the Comptroller of the Currency, Treasury (OCC); the Federal Reserve; and the Federal Deposit Insurance Corporation (FDIC) issued a Notice of Proposed Rulemaking that would require financial institutions to notify their primary federal financial regulator, within 36 hours of becoming aware, that a “computer-security incident” or “notification incident” has occurred. The rule would also require bank service providers to notify “at least two individuals at affected banking organization customers immediately after the bank service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided for four or more hours.” The text of the Notice of Proposed Rulemaking, titled “Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers” (the Proposed Notice Rule), can be found [here](#). Interested parties are encouraged to submit comments to the Proposed Notice Rule within 90 days after the date of publication in the Federal Register.

The Proposed Notice Rule is intended to provide federally regulated financial institutions and their service providers clarity as to what constitutes a noticeable computer-security incident and when the 36-hour notice is triggered. The Proposed Notice Rule is unique in that it is focused on security events that disrupt financial institutions’ overall operations, rather than security events that impact customer information.

1. Noticeable Computer Security Incident: Financial institutions would be required to notify their primary federal regulator in the event of a computer-security incident that the financial institution “believes in good faith could materially disrupt, degrade, or impair the ability of the banking organization 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; any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or those operations of a banking organization, 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.”

The Proposed Notice Rule defines “computer-security incident” as an occurrence that “(i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or (ii) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”

The federal financial regulators explained in the Supplementary Information section of the Proposed Notice Rule that not all computer-security incidents require a banking organization to notify its primary federal regulator; only those that rise to the level of notification incidents require notification. According to the regulators, “[o]ther computer-security incidents, such as a limited distributed denial of service attack that is promptly and successfully managed by a banking organization, would not require notice to the appropriate agency.” The regulators also provided a “a non-exhaustive list of events that would be considered ‘notification incidents’ under the proposed rule: (1) Large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time (e.g., more than 4 hours); (2) A bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and recovery time is undeterminable; (3) A failed system upgrade or change that results in widespread user outages for customers and bank employees; (4) An unrecoverable system failure that results in activation of a banking organization’s business continuity or disaster recovery plan; (5) A computer hacking incident that disables banking operations for an extended period of time; (6) Malware propagating on a banking organization’s network that requires the banking organization to disengage all Internet-based network connections; and (7) A ransom malware attack that encrypts a core banking system or backup data.” Although not in the text of the Proposed Notice Rule itself, the criteria cited in the Supplementary Information section do provide banks with helpful guidance moving forward.

2. 36-Hour Notice Trigger: Financial institutions would be required to report a notification incident to their primary federal regulator “as soon as possible and no later than 36 hours after the banking organization believes in good faith that a notification incident has occurred.” The Supplementary Information section clarifies that the regulators “do not expect that a banking organization would typically be able to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident. Rather, the agencies anticipate that a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident. In this context, the agencies recognize banking organizations may not come to a good faith belief that a notification incident has occurred outside of normal business hours. Only once the banking organization has made such a determination would the requirement to report within 36 hours begin.”

Service providers of federally regulated financial institutions would be required to notify “at least two individuals at each affected banking organization customer immediately after the bank service provider 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 (12 U.S.C. 1861–1867) for four or more hours.” As to why service providers would be

required to notify “at least two individuals,” the regulators stressed that the requirement would help to ensure that “banking organizations provide timely notice of significant computer-security incident disruptions to the agencies.”

The Proposed Notice Rule follows similar rules enacted by state financial regulators in recent years. For example, the New York Department of Financial Services’ (NY DFS) [2017 Cybersecurity Regulation](#) requires covered entities to notify the NY DFS of certain “Cybersecurity Events” “as promptly as possible, but in no event later than 72 hours from a determination that a reportable Cybersecurity Event has occurred.” The NY DFS regulation defines a reportable “Cybersecurity Event” as one that “falls into at least one of the following categories: (1) the Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (2) the Cybersecurity Event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.”

Federally regulated banks already have notice obligations under relevant federal financial regulations. For example, under the reporting requirements of the Bank Secrecy Act (BSA) and its implementing regulations, certain banking organizations are required to file Suspicious Activity Reports when they detect a known or suspected criminal violation of federal law or a suspicious transaction related to money-laundering activity. Likewise, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, which interprets section 501(b) of the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines Establishing Information Security Standards, generally sets forth the supervisory expectation that a banking organization notify its primary federal regulator “as soon as possible” if the organization becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information.

The federal financial regulators reasoned that the current rules in place are “too narrow in scope to address all relevant computer-security incidents that would be covered by the proposed rule.” The regulators added that “in particular, the GLBA notification standard focuses on incidents that result in the compromise of sensitive customer information and, therefore, does not include the reporting of incidents that disrupt operations but do not compromise sensitive customer information.”

Authors



Franca Harris Gutierrez

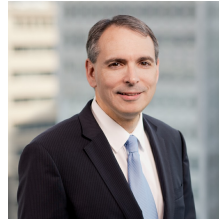
PARTNER

Chair, Financial Institutions Practice

Co-Chair, Securities and Financial Regulation Practice

✉ franca.gutierrez@wilmerhale.com

☎ +1 202 663 6557



Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

✉ benjamin.powell@wilmerhale.com

☎ +1 202 663 6770



Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice

Co-Chair, Cybersecurity and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



Reade Jacob

COUNSEL

✉ reade.jacob@wilmerhale.com

☎ +1 202 663 6330