Cyber Incident Notification Requirements for Banking Organizations and Service Providers – Proposed Rule
Five Things To Know

On December 18, 2020, the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation (collectively, the "agencies") issued a notice of proposed rulemaking ("proposal") requiring a banking organization to notify its primary federal regulator within 36 hours of a significant cybersecurity incident and requiring a bank service provider to notify at least two individuals at an affected banking organization customer of a significant cybersecurity incident that could disrupt services for four or more hours. The proposed rule's notification requirement is intended to provide an early alert to the banking organization's regulator of emerging threats to the banking organization and the broader financial system.

The agencies are requesting comments on all aspects of the proposal and on 16 specific questions in the proposal. Comments will be due 90 days after the proposal's publication in the Federal Register.

1 The proposal would require notification for only the most significant cybersecurity incidents.

The proposal would require a banking organization (e.g., a bank, savings association, depository institution holding company, or U.S. operation of a foreign banking organization such as a U.S. branch or agency office) to notify its primary federal regulator of any "computer-security incident" that rises to the level of a "notification incident."

- A "computer-security incident" would be defined as "an occurrence that (i) results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that 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."
- A "notification incident" would be defined as "a computer-security incident that a banking organization believes in good faith could materially disrupt, degrade, or impair (i) [t]he 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; (ii) [a]ny 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 (iii) [t]hose 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 proposal would require notification to the primary federal regulator as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred. In addition, the proposal would require the banking organization to alert any parent company that is itself a banking organization to the occurrence of the notification incident, and the parent banking organization would need to make a separate assessment of whether the incident requires reporting to the parent's primary federal regulator. In addition, if a notification incident occurs at a banking organization's subsidiary that is not itself a banking organization, the banking organization would be required to assess whether the incident requires notice to the organization's primary federal regulator, but the non-bank subsidiary would not have its own notification requirement under the proposal.

Examples of reportable notification incidents, as enumerated in the proposal, include a large-scale distributed denial of service attack that disrupts customer account access for an extended period of time, a failed system upgrade or change that results in widespread user outages, an unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan, a computer hacking incident that disables banking operations for an extended period of time, malware propagating on a banking organization's network that requires the banking organization to disengage all internet-based network connections, and a ransom malware

attack that encrypts a core banking system or backup data. The agencies estimate that only about 150 incidents each year would meet the significance threshold for the notification requirement.

---

2 The proposal would not prescribe requirements for the contents of a notice to be provided to the regulator.

Because notification is intended to serve only as an early alert and not to provide an assessment of the incident, the proposal states that the agencies would not require specific information to be included in the notice nor would they require any prescribed reporting forms or templates. The proposal indicates that the agencies would expect only that banking organizations share "general information about what is known at the time." In addition, notice could be provided through any form of written or oral communication, including through any technological means, to a designated point of contact identified by the banking organization's primary federal regulator.

---

3 Bank service providers would be required to notify affected banking organizations of significant cybersecurity incidents.

The proposal would require a bank service provider 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 under the Bank Service Company Act ("BSCA") to the banking organization for four or more hours. The bank service provider would not be expected to assess whether the incident rises to the level of a notification incident for the banking organization customer; rather, this assessment would be the customer's responsibility.

---

4 The proposal is intended to fill gaps in the current framework for cybersecurity incident notifications.

The proposal highlights that banking organizations currently are required to report certain instances of disruptive cyber-events and cyber-crimes by filing a Suspicious Activity Report ("SAR"). However, SARs do not require the reporting of every incident captured by the proposed definition of "notification incident." Moreover, most SARs are required to be filed within 30 calendar days of the initial detection of facts that may constitute a basis for filing a report and therefore do not provide the agencies with timely notice.

In addition, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice and the Interagency Guidelines Establishing Information Security Standards require a banking organization to notify its primary federal regulator "as soon as possible" if it becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information. The proposal covers a broader range of incidents, including incidents that disrupt operations or systems but do not compromise sensitive customer information.

Finally, the BSCA requires a banking organization to notify the appropriate federal banking agency of the existence of a relationship with a service provider, but the act does not contain a notification requirement if the service is disrupted.

5 The proposal's notification thresholds are designed to be consistent with concepts used in resolution planning under the Dodd-Frank Act.

The second and third prongs of the "notification incident" definition are intended to be consistent with the meanings of the terms "core business line" and "critical operation" under resolution planning regulations adopted by the Federal Reserve Board and Federal Deposit Insurance Corporation pursuant to section 165(d) of the Dodd-Frank Act. Banking organizations that are subject to the resolution plan regulations may use the core business lines and critical operations identified in their resolution plans to identify incidents that require reporting under the second and third prongs.

For further information or details on this topic, please contact:

Randy Benjenk
Washington
+1 202 662 5041
rbenjenk@cov.com

Jeremy Newell
Washington
+1 202 662 5569
jnewell@cov.com

Michael Nonaka
Washington
+1 202 662 5727
mnonaka@cov.com

Karen Solomon
Washington
+1 202 662 5489
ksolomon@cov.com

James Garland
Washington
+1 202 662 5337
jgarland@cov.com

Micaela McMurrough
New York
+1 212 841 1242
mmcmurrough@cov.com

Ashden Fein
Washington
+1 202 662 5116
afein@cov.com

Devika Singh
Washington
+1 202 662 5689
dsingh@cov.com