Articles + Publications | December 2, 2021

Think Fast: Banking Regulators Release Final Computer-Security Incident Notification Requirements

WRITTEN BY

Ronald Raether, Jr. | James W. Stevens | Graham T. Dean

Introduction

On November 18, federal banking agencies[1] issued the long-awaited final rule,[2] establishing data security incident response notification requirements for "banking organizations" and "bank service providers" (terms defined below). Included in this rule is a headline-grabbing 36-hour regulatory notification requirement for banking organizations. This final rule is set to take effect on April 1, 2022, and entities are required to comply by May 1, 2022. Covered entities should begin analyzing their breach response procedures now to ensure timely compliance.

Final Rule Requirements

The final rule includes notice requirements between (1) banking organizations and their regulators, and (2) bank service providers and their banking organization customers. The following defined terms are important to understanding what is required under this rule:

- ***Banking Organization***
  - The definition of banking organization differs based on the applicable federal regulator:
    - **FDIC:** Banking organization means an FDIC-supervised insured depository institution, including all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured state savings associations.
    - **OCC:** Banking organization means a national bank, federal savings association, or federal branch or agency of a foreign bank.
    - **Federal Reserve:** Banking organization means a U.S. bank holding company, U.S. savings and loan holding company, state member bank, the U.S. operations of foreign banking organizations, and an edge or agreement corporation.
  - ***Bank service provider*** means a bank service company or other person that performs covered services provided.

- ***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.

- ***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:

  - (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 operations, 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.

Banking Organization Notification to Agencies

Banking organizations must provide notice to their applicable regulator "as soon as possible" and no later than "36 hours after the banking organization determines that a notification incident has occurred." Based on the regulator, there are subtle differences regarding the details of these notifications; however, as a general matter these notifications must be made to the agency's "designated point of contact" via email, telephone, or "other similar methods."

The timing aspect of this notice requirement is quite short as compared to other data protection laws. For example, the EU's General Data Protection Regulation (GDPR) requires notice "without undue delay, but no later than 72 hours after becoming aware of the data incident."[3] In addition, many U.S. state data breach laws require notification anytime within a period of 30 days. The shortest state notification period is found in the Illinois law, which requires that notification be made within 72 hours if a breach affects more than 250 residents' personal information.

While the final rule's timing requirement is shorter than other breach laws, the regulatory burden of this requirement on banking organizations is made somewhat uncertain by the definition of "notification incident." Notice does not depend on the nature of the information at issue, but instead is limited to incidents that have disrupted or degraded, or are reasonably likely to "materially disrupt or degrade," the banking organization's (1) ability to provide services, (2) business lines, or (3) operations (see definition above for precise wording). In the definition of notification incident, all three of these points are limited by qualifying statements. For instance, a disruption to the banking organization's operations is only reportable if "the failure or discontinuance" poses "a threat to the financial stability of the United States." Much like the threat of consumer harm triggered in state breach notification laws, the contours of when an incident requires notice (*e.g.,* is materially disruptive) will likely be defined over time and through experience.

It is also important to note that the 36-hour notification period does not start until the banking organization "determines that a notification incident has occurred." Other breach notification laws start the clock at an earlier

stage in the breach investigation/remediation process. For instance, the 72-hour window for regulatory notifications under GDPR opens as soon as an entity "become[s] aware" of a breach." Collectively, this "determination" that a notification incident has occurred and the aforementioned qualifying statements in the definition of "notification incident" soften an otherwise harsh timing requirement.

Bank Service Provider Notifications to Banking Organization Customers

Bank service providers also are required to notify "at least one bank-designated point of contact at 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 materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade covered services provided to such banking organization for four hours or more." It is important to note that the definition of "computer-security incident" is much broader than "notification incident"; therefore in practice, these notifications may occur much more frequently than the regulatory notifications described above. However, the effect of this rule may be limited as most service provider contracts already require notice, and in many cases, this notice is triggered by less significant data incidents. For those that do not, amendments may be in order.

There is no specific deadline for bank service providers; however, the final rule does require that the service provider notify their banking organization's "designated point of contact" "as soon as possible." The bank-designated point of contact is any email, phone number, or other contact provided by the banking organization. If a point of contact has not been provided, the notification should be provided to the bank organization's chief executive officer and chief information officer or "two individuals of comparable responsibilities through any means."

Current Cyber Incident Reporting Requirements

While this rule provides the clearest and most comprehensive cyber incident reporting requirements to date, there are applicable existing laws that may require notification after a cyber incident. Notably, under the Gramm-Leach-Bliley Act and the Interagency Guidelines Establishing Information Security Standards, federal regulators must be notified "as soon as possible" following unauthorized access to, or use of, sensitive customer information. Furthermore, the Bank Secrecy Act requires that banks file a "suspicious activity report" when they detect criminal activity. These reports must be filed within 30 days or "as soon as possible" if the incident involves "unauthorized access to or use of sensitive customer information." In the supplementary information for the proposed version of this rule,[4] the agencies note that these "current reporting requirements related to cyber incidents are neither designed nor intended to provide timely information to regulators regarding such incidents." In addition to these federal requirements, every state has breach notification requirements of its own. While each state breach notification law is unique, the states' laws generally require that consumers and state-level regulators be notified in certain instances. Many states only require notification if there is a risk of harm to the consumers, and do not include specific timing requirements.

Conclusion

Banking organizations and bank service providers must ensure that they have the plans, policies, and procedures in place to comply with these requirements. As a part of these compliance efforts, covered entities should

consider: (1) updating incident response plans to include the appropriate points of contact, (2) conducting training exercises in accordance with these new timing requirements, (3) incorporating the applicable definitions into service provider contracts, and (4) updating/drafting incident response playbooks. Furthermore, banking organizations and bank service providers must remain cognizant of other applicable state, federal, and international security incident reporting requirements. Troutman Pepper's privacy professionals have extensive, applicable compliance experience and are ready to help businesses navigate this difficult regulatory environment.

---

[1] Including the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC).

[2] *See* https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

[3] Regulation (EU) 2016/679, Art. 33.

[4] *See* https://www.federalregister.gov/documents/2021/01/12/2020-28498/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

RELATED INDUSTRIES + PRACTICES

- Financial Services
- Privacy + Cyber