Cullen | Dykman

Federal Banking Regulators Mandate Report of Major Cyber Incidents within 36 Hours

December 1, 2021

The Federal Deposit Insurance Corporation ("FDIC"), the Board of Governors of the Federal Reserve System ("Board"), and the Office of the Comptroller of the Currency ("OCC") (collectively, the "Agencies") issued a final rule requiring banking organizations[1] such as federal or state-chartered banks and savings associations to notify their primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after the banking organization determines that such incident has occurred.

Additionally, bank service providers[2] 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 it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade covered services[3] provided to such banking organization customer for four or more hours.

The final rule is effective April 1, 2022, but the Agencies have provided a compliance date of May 1, 2022 to provide additional time to implement the final rule. The primary focus of this advisory is the 36 hour-notification requirement for banking organizations. Please see a detailed discussion set forth below.

Definition of Notification Incidents

A banking organization is required to report a "notification incident." 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: (i) 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; (ii) 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 (iii) 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.

Examples of Notification Incidents

The following is a non-exhaustive list of notification incidents that generally need to be reported under the final 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 banking organization 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 on a banking organization's network that poses an imminent threat to the banking organization's core business lines or critical operations or that requires the banking organization to disengage any compromised products or information systems that support the banking organization's core business lines or critical operations from Internet-based network connections; and
7. A ransom malware attack that encrypts a core banking system or backup data.

The final rule requires banking organizations to consider, on a case-by-case basis, whether any significant computer-security incidents they experience constitute notification incidents for purposes of notifying the appropriate agency. If a banking organization is in doubt as to whether it is experiencing a notification incident for purposes of notifying its primary federal regulator, such banking organization is advised to contact its regulator. The final rule also provides that the Agencies do not expect to take supervisory action when a banking organization files a notification upon a mistaken determination that a notification incident has occurred.

Timing of Notification

Notwithstanding comments requesting the Agencies to extend the 36-hour time frame, the Agencies continue to believe that "36 hours is the appropriate timeframe, given the simplicity of the notification requirement and the severity of incidents captured by the definition of 'notification incident.'"

The 36-hour clock starts once a banking organization has determined that a notification incident has occurred. A banking organization is not required to determine that a notification incident has occurred immediately upon becoming aware of a computer-security incident. The Agencies anticipate that a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident.

Method of Notification

A banking organization must notify the appropriate supervisory office, or a designated point of contact, about a notification incident through email, telephone, or other similar methods that the supervisory agency may prescribe.

No Content or Format Requirements for the Notification

There is no specific content or format requirement for the notice of a notification incident. This is because the final rule is designed to ensure that the appropriate agency receives timely notice of significant emergent incidents, while providing flexibility to the banking organization to determine the content of the notification.

Cybersecurity Event Notification Requirement under New York State Law

In addition to this new notification to the federal banking regulators, New York State financial institutions[4] should continue to be aware of their obligations under the New York State cybersecurity notification requirements. Pursuant to the New York State Department of Financial Services ("NYDFS") Regulation Part 500, subject to limited exemptions[5], most New York State-chartered banks and NYDFS regulated financial organizations must notify the NYDFS no later than 72 hours after determining that a cybersecurity event either has: (i) impacted the entity and notice is required to be provided to another regulator, or (ii) a reasonable likelihood of materially harming a material part of the normal operation of the entity. Our earlier guidance on Part 500 of the NYSDFS regulations is available here .

Additionally, unless otherwise exempt[6], if the cybersecurity incident involves private information of consumers, those consumers who have been affected by cybersecurity incidents must also be notified pursuant to New York General Business Law Section 899-aa.

Additional Information

A copy of the final rule is available here. Please note that this advisory is a general overview of the final rule and is not intended as legal advice. If you have any questions regarding the final rule or notification requirements in general, please feel free to contact Joseph D. Simon at (516) 357-3710 or via email at jsimon@cullenllp.com, Kevin Patterson at (516) 296-9196 or via email at kpatterson@cullenllp.com, Elizabeth A. Murphy at (516) 296-9154, or via email at emurphy@cullenllp.com, or Mandy Xu at (516) 357-3850 or via email at mxu@cullenllp.com.

Footnotes

[1] For the OCC, "banking organizations" includes national banks, federal savings associations, and federal branches and agencies of foreign banks. For the Board, "banking organizations" 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. For the FDIC, "banking organizations" includes all insured state nonmember banks, insured state-licensed branches of foreign banks, and insured State savings associations. Each agency's definition excludes a financial market utility (FMU) designated under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

[2] "Bank service provider" means a company or person that performs services for a banking organization that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867). This definition excludes an FMU which is "any person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person." 12 U.S.C. 5462(6).

[3] Covered services are services performed, by a person, that are subject to the Bank Service Company Act (12 U.S.C. 1861–1867). Covered services include, but are not limited to, check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar

functions.

[4] Any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York Banking Law, the Insurance Law or the Financial Services Law is a Covered Entity subject to the New York State cybersecurity requirements.

[5] There is an exemption for an entity with less than 10 employees or less than $5,000,000 in gross annual revenue in each of the last 3 fiscal years from New York business operations of the Covered Entity and its Affiliates. A Covered Entity that qualifies for any exemptions must file a Notice of Exemption within 30 days of the determination that the Covered Entity is exempt.

[6] Notice to affected consumers is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials.

Practices

- Regulatory and Compliance

Attorneys

- Joseph D. Simon
- Kevin Patterson
- Elizabeth A. Murphy