VedderPrice

Federal Bank Regulators Expand Duty to Notify after a Cybersecurity Event

By James M. Kane, James W. Morrissey, Daniel C. McKay, II, Jennifer Durham King, Juan M. Arciniegas, Mark C. Svalina and Mary Donohue

December 17, 2021

On November 18, 2021, the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Board of Governors of the Federal Reserve System (FRB) (each, an "Agency" and, collectively, the "Agencies") finalized a uniform regulation, codified at 12 C.F.R. Part 53, 12 C.F.R. Part 225.300 and 12 C.F.R. Part 304, with the stated purpose of improving the sharing of information about cybersecurity incidents harmful to the U.S. banking system (the "Regulation"). Pursuant to the Regulation, banks will be required to notify their primary federal regulatory Agency within thirty-six (36) hours of "any significant computer-security incident."

What is the purpose of the Regulation?

The Regulation fills an existing gap among federal regulations, including current requirements existing under the Bank Secrecy Act and other anti-money laundering regulations, the Gramm-Leach Bliley Act and the Bank Service Company Act, which presently do not impose direct cybersecurity incident reporting requirements for banking organizations.

When is the Regulation effective?

While the Regulation has an effective date of April 1, 2022, compliance is required by May 1, 2022.

Who is impacted?

The Regulation is applicable to bank holding companies, savings and loan holding companies, national banking associations, state-chartered banks, federal and state savings associations/thrifts and federal and state branches of foreign banks, and to their service providers (collectively hereinafter, a "bank" or "banks").

What needs to be reported?

Banks will need to consider, on a case-by-case basis, whether any significant computer-security incidents constitute notification incidents for the purposes of reporting. Below is a non-exhaustive list of incidents that generally need to be reported:

(i) large-scale distributed denial of service attacks that disrupt customer account access for an extended period of time;

(ii) 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;

(iii) a failed system upgrade or change that results in widespread user outages for customers and banking organization employees;

(iv) an unrecoverable system failure that results in activation of a banking organization's business continuity or disaster recovery plan;

(v) a computer hacking incident that disables banking operations for an extended period of time;

(vi) malware on a bank's network that poses an imminent threat to the bank's core business lines or critical operations or that requires the bank 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

(vii) a ransom malware attack that encrypts a core banking system or backup data.

When must a bank report a covered event?

Pursuant to the Regulation, banks will be required to notify their primary federal regulatory Agency of "any significant computer-security incident" within thirty-six (36) hours after the bank has determined a notification incident has occurred. The Regulation, however, does not address directly when a bank is deemed to have "determined" that a notification incident has occurred. The Agencies have noted that the incident does not need to be immediately discovered, but they anticipate that discovery of an incident will be made within a reasonable amount of time. The Agencies have noted that some incidents may occur outside of normal business hours, and only once the banking organization has made such a determination would the timeframe begin. The Agencies encourage same-day notification to their primary federal regulator.

As is current practice, the notification must be made to the appropriate supervisory office or point of contact at the applicable Agency, and the Regulation does not specify content or format requirements for the notice. Notifications are to be made to the Agency point of contact by telephone or email.

What should banks being doing now to prepare for the Regulation?

In the interim, banks should review internal policies and procedures to ensure a reporting procedure is in place to comply with the May 1, 2022 compliance deadline.

We note that state-chartered banks should keep in mind that certain states, such as New York, have implemented similar reporting requirements. State-level reporting obligations may differ from the Regulation and other federal reporting requirements.

Existing Regulatory Requirements

The new Regulation fills a gap that is not covered by guidance on information security (the "Security Guidelines"). Specifically, the existing interagency Security Guidelines require notice to the appropriate regulator only if certain customer information was compromised and if a bank determined there was a likelihood the information would be misused. The Security Guidelines, codified at 12 C.F.R. Part 30, Appendix B, 12 C.F.R. Part 208, Appendix D-2 and 12 C.F.R. Part 364, Appendix B, remain in effect and direct every financial institution to assess the following risks, among others, when developing its information security program:

a. reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

b. the likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and

c. the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

Following the assessment of these risks, the Security Guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including the following:

a. access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals;

b. background checks for employees with responsibilities for access to customer information; and

c. response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.

The Security Guidelines impose requirements for a response program, including (i) an assessment of the nature and scope of an incident and types of customer information that have been accessed or misused, (ii) notifying the primary federal regulatory Agency as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information and (iii) notifying appropriate law enforcement authorities, in addition to timely filing a Suspicious Activity Report in situations involving federal criminal violations requiring immediate attention.

The Regulation established as of November of this year targets general security breaches and cyberattacks, and is not limited to incidents involving a compromise of customer information and the likely misuse of such information addressed in the Security Guidelines. As a result, the Regulation is intended to work with already existing regulatory obligations to ensure that banks are properly addressing cybersecurity threats.

To view the full text of the Regulation, click here.

If you have any questions regarding the topics discussed in this article, please contact **James M. Kane** at jkane@vedderprice.com, **James W. Morrissey** at jmorrissey@vedderprice.com, **Daniel C. McKay, II** at dmckay@vedderprice.com, **Jennifer Durham King** at jking@vedderprice.com, **Juan M. Arciniegas** at jarciniegas@vedderprice.com, **Mark C. Svalina** at msvalina@vedderprice.com, **Mary Donohue** at mdonohue@vedderprice.com or any Vedder Price attorney with whom you have worked.