PUBLICATION

NCUA Approves New Cyber Incident Reporting Requirements: What Credit Unions Need to Know

Authors: Alexander Frank Koskey, III, Matthew George White
February 27, 2023

The National Credit Union Administration (NCUA) has approved new cyber incident reporting requirements for credit unions. Under the final rule, federally insured credit unions will be required to notify the NCUA of a "reportable cyber incident" within 72 hours of such an event. The NCUA's final rule follows the 36-hour notification requirement implemented for banking organizations last year. While the final rule doubles the reporting time for credit unions, it also could require credit unions to notify the NCUA of a significantly broader set of incidents than required for banking organizations. The final rule continues the trend of regulators increasing their focus on the cybersecurity safeguards among financial institutions and, in particular, of requiring faster notifications when incidents occur.

The final rule will go into effect on September 1, 2023. This alert contains a primer about the rule and proactive steps credit unions should be taking in anticipation of these new reporting requirements.

What is a Reportable Cyber Incident?

The rule requires credit unions to notify the NCUA no later than 72 hours after it reasonably believes a reportable cyber incident has occurred. A reportable cyber incident is defined as any substantial cyber incident that leads to:

- A substantial loss of confidentiality, integrity, or availability of a network or member information system that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes;
- A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities; and/or
- A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union service organization, cloud service provider, managed service provider, or other third-party data hosting provider or a supply chain compromise.

Examples of Reportable Incidents

The NCUA's final rule contained some examples of what may constitute a reportable cyber incident, including, without limitation:

- If a member information system has been unlawfully modified and/or sensitive data has been left exposed to an unauthorized person, process, or device;
- A failed system upgrade or change that results in unplanned widespread user outages for credit union members and employees; or
- A distributed denial of service (DDoS) attack that disrupts member account access.

The rule does state that incidents such as unsuccessful malware attacks or failed attempts to gain access to systems do not have to be reported. In addition, third-party incidents that are unknown to a credit union and hold information about individuals who happen to be credit union members or employees do not impose a notification requirement.

How Should Incidents Be Reported?

According to the final rule, incidents may be reported to the NCUA "via email, telephone, or other similar methods that the NCUA may prescribe." The reporting methods are designed to give credit unions flexibility based upon the impact of a potential cyber incident. The NCUA has also stressed that an initial report does not have to include a full assessment of the incident.

Next Steps for Credit Unions

The NCUA will be providing additional guidance, including examples of reportable and non-reportable incidents, before the final rule becomes effective in September. In the meantime, credit unions should be reviewing and updating their incident response plans and vendor management programs to ensure that they are prepared to comply with these enhanced requirements.

If you have any questions concerning these issues, or any aspect of your cybersecurity or privacy programs, please contact Alex Koskey or Matt White, co-chairs of Baker Donelson's Financial Services Cybersecurity and Data Protection Team, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.