LEWIS ROCA

NCUA APPROVES 72-HOUR BREACH NOTIFICATION RULE

By John Gray, CIPP/US and Patrick McCormick, CIPP/US on 03/7/2023
Posted in Cybersecurity and Data Protection

The National Credit Union Administration (NCUA) approved a final rule that will require any Federally-Insured Credit Union (FICU)—including federally chartered corporate credit unions and federally insured state-chartered corporate credit unions—to report certain cyber incidents to the NCUA as soon as possible, and no later than 72 hours, after it "reasonably believes" it has experienced a reportable incident. The rule, which adds a new subsection (c) to 12 CFR Part 748.1, goes into effect September 1, 2023.

In issuing its new rule, the NCUA attempted to closely follow the terminology and reporting framework set forth in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which will likely go into effect in 2025. For example, the new NCUA rule includes definitions of "cyber incident" and "reportable cyber incident" that are similar to the definitions set forth in CIRCIA. The NCUA rule is not identical to CIRCIA, though, and FICUs should not necessarily rely on compliance with one to ensure compliance with the other.

The new NCUA rule also shares some similarities with the cyber-incident notification rule for banks that took effect in April 2022, but it contains a number of differences, as well, including three distinctions of particular note. First, the NCUA rule requires a report within 72 hours, while the banking rule requires a report within 36 hours. Second, the NCUA rule starts the clock when a FICU "reasonably believes" an incident has occurred, while the banking rule starts its clock once a banking organization "determines" that an incident has occurred. Third, the NCUA rule requires a report of any "substantial" incident or compromise, while the banking rule only requires reporting in the event of "actual harm."

Finally, the NCUA expressly stated that its new rule does not impact existing contractual relationships and does not require a FICU to amend its existing contracts with third parties to comply with the rule. Nonetheless, FICUs may want to examine their contractual reporting obligations to identify any inconsistencies between those obligations and the obligations imposed by the new NCUA rule.

Please contact Patrick Emerson McCormick, CIPP/US or another member of Lewis Roca's Data Protection and Cybersecurity team for more information about the NCUA rules and other federal privacy and cybersecurity laws that may affect your organization.

Tags: Data Protection and Cybersecurity