On July 27, 2022, the National Credit Union Administration (NCUA) issued a proposed rule requiring federally insured credit unions (FICUs) to notify the NCUA within seventy-two (72) hours of discovering a reportable cyber incident.

**Summary of the Proposed Rule**

Under existing federal law (the Interagency Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice), credit unions must
notify the appropriate NCUA Regional Director, and, in the case of state-chartered credit unions, their state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information.

If finalized, the new rule will require FICUs to report to the NCUA, as soon as possible and no later than 72 hours, substantial cyber incidents leading to any of the following:

(A) 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.

(B) A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.

(C) 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, or other third-party data hosting provider or by a supply chain compromise.

The proposed rule defines reportable cyber incidents to encompass “substantial” cyber incidents. Whether a particular cyber incident is considered substantial will likely depend on a variety of factors, including the size of the FICU, the type of incident and impact of loss, and the incident’s duration.

Notably, the proposed rule’s definition of a reportable cyber incident is broader than that included in the 36-hour cyber incident reporting rule for federally regulated banking organizations that went into effect May 1, 2022, which requires notice to federal regulators following discovery of ransomware or certain disruptive cybersecurity incidents. The NCUA’s proposed rule also applies to certain incidents that result in unauthorized access to broadly defined sensitive data.

The proposed notification requirement is intended to provide an early alert to the NCUA and does not require FICUs to provide within the 72-hour time period a detailed incident assessment to the NCUA. Rather, the report should include, for example, the date and a basic description of the incident, affected functions, exploited vulnerabilities, and/or any known information regarding the threat actor.

A full text of the proposed rule can be found here.

Comments on the Proposed Rule

All comments on the proposed rule are due to the NCUA by September 26, 2022.

© Polsinelli PC, Polsinelli LLP in California

National Law Review, Volume XII, Number 214