NASCUS
The National Association of State Credit Union Supervisors

NASCUS Comments: Cyber Incident Notification Requirements for Federally Insured Credit Unions

September 26, 2022

Melane Conyers-Ausbrooks
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314

Re: Cyber Incident Notification Requirements for Federally Insured Credit Unions (RIN 3133-AF47)

Dear Secretary Conyers-Ausbrooks:

The National Association of State Credit Union Supervisors (NASCUS)[1] submits this letter in response to the National Credit Union Administration's (NCUA) notice of proposed rulemaking and request for comment regarding RIN 3133-AF47, Cyber Incident Notification Requirements for Federally Insured Credit Unions.[2]

The proposal would require a federally insured credit union (FICU) to notify NCUA as soon as possible and no later than 72 hours after the FICU reasonably believes that it has experienced a "reportable cyber incident."

NCUA's proposed rule represents a reasonable balance between the need for regulators to be made aware of potential significant disruption in financial services and an institution's need to focus on mitigation of the effects of a cyber-related disruption. NASCUS supports this rulemaking and submits the following recommendations for NCUA's consideration.

Coordination and Cohesion with Other State and Federal Cybersecurity Reporting Requirements

While NASCUS supports the proposed rulemaking, we note that credit unions have numerous reporting requirements related to a material cyber incident. In some cases, state-specific laws related to data security and privacy may trigger reporting, depending

[1] NASCUS is the professional association of the nation's forty-five state credit union regulatory agencies that charter and supervise over 1900 state credit unions. NASCUS membership includes state regulatory agencies, state chartered and federally chartered credit unions, and other important stakeholders in the state system. State-chartered credit unions hold over half of the $2.2 trillion assets in the credit union system and are proud to represent nearly half of the 129 million members.

[2] Fed. Reg. Vol 87 No. 143, p 45029

on the nature and scope of the incident Suspicious Activity Report (SAR) filing may be required, compliance with Appendix B, Part 748 regarding unauthorized access to member data, and pending guidelines related to cyber incident reporting from the Cybersecurity and Infrastructure Security Agency. NASCUS recommends that NCUA closely coordinate with state and federal regulators to ensure NCUA reporting requirements align and cohere with the broader cyber incident reporting framework to minimize redundancy and inconsistency that could otherwise divert credit union resources needed to respond to and mitigate the underlying incident.

Definitions

The proposal defines both "cyber incident" and "reportable cyber incident". To determine if the incident is a "reportable cyber incident", a credit union would first need to determine whether the incident fits the definition of "cyber incident." If so, then the credit union would further evaluate if the incident falls within the "reportable" cyber incident category according to NCUA's proposed definitions.[3] NASCUS commends NCUA for including a list of examples of incidents that would be considered "reportable" under the proposed rule. The examples provided by NCUA help clarify how certain incidents might be evaluated in the context of the reporting requirements. We recommend NCUA commit to regularly updating the list of examples as a resource for credit unions to provide further clarity to the industry.

Reporting of a Cyber Incident and Mechanism for Reporting

The proposed rule provides credit unions with the basic information the agency expects to be reported, to the extent it is known to the FICU at the time of reporting, as well as the timeframe of 72 hours once an institution has formed a reasonable belief, they have experienced a reportable incident. NASCUS believes the 72-hour timeframe strikes a reasonable balance providing institutions time to notify the agency while also implementing their mitigation plans.

The NCUA indicates they expect there will be further follow-up communications between a reporting FICU and the agency through the supervisory process, as needed.

While the NCUA believes requesting the basic information for the initial report will be of minimal burden to credit unions, a prescribed format would be beneficial to the industry and NCUA to meet the proposal's intended purpose to promote early awareness of emerging threats. A consistent format and dedicated means of reporting, similar to that prescribed by the banking agencies[4], would aid the industry and NCUA in addressing emerging threats in a timely manner.

[3] Fed.Reg.Vol. 87, No.143, p. 45030

[4] See FDIC FIL-12-2022, Federal Reserve SR 22-4/CA 22-3, OCC Bulletin https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-8.html2022-8

Industry Communication

While outside the scope of the proposed rulemaking, NASCUS recommends NCUA give careful consideration to ways to improve cyber incident-related communication with state regulators and credit unions. From a systemic perspective, early warning of a coordinated, or unusually sophisticated singular event could be vital in ensuring adaptive hardening of cybersecurity protocols.

Policy Expectations

As previously stated, NCUA has indicated additional follow-up on a reportable cyber-incident is expected through the supervisory process. During the supervisory process, the state supervisory authority and NCUA review a FICU's policies and procedures. As with any amendments to regulation, there are often policy expectations. NCUA should clearly define what is expected in a FICU's policy and issue supervisory guidance for institutions to review in developing their policies and procedures applicable to cyber-incident reporting.

Conclusion

We thank the NCUA for the opportunity to submit the above comments for consideration in the development of a final rule for cyber-incident reporting. Cyber incidents have become one of the most significant threats to the financial services industry and we commend the NCUA for its efforts in the development of rulemaking to combat the growing concern. We encourage the NCUA to continue working with state supervisory authorities in order to avoid additional burdens on federally insured state-chartered credit unions.

Sincerely,

- Signature redacted for electronic publication –

Sarah Stevenson
Vice President, Regulatory Affairs
NASCUS