

# Cooperative Credit Union Association

Delaware • Massachusetts • New Hampshire • Rhode Island

*Creating Cooperative Power*

September 26, 2022

Ms. Melane Conyers-Ausbrooks  
Secretary of the Board  
National Credit Union Administration  
1775 Duke Street  
Alexandria, VA 22314-3428

## **RE: Cooperative Credit Union Association, Inc. Comments on Proposed Rule on Cyber Incident Notification Requirements for Federally Insured Credit Unions (RIN 3133-AF47)**

Dear Ms. Conyers-Ausbrooks,

On behalf of its member credit unions, the Cooperative Credit Union Association, Inc. (“Association”) appreciates the opportunity to comment on the National Credit Union Administration’s (NCUA) proposed rule on Cyber Incident Notification Requirements for Federally Insured Credit Unions. The Association is the state trade association representing approximately 200 state and federally-chartered credit unions located in the states of Delaware, Massachusetts, New Hampshire, and Rhode Island, which further serve over 3.6 million consumer members. The Association has developed these comments in consultation with our members.

### **The Association’s High-Level Comments**

- The Association supports NCUA’s proposal to update its Part 748 rules so that credit unions experiencing a cyber intrusion must provide NCUA with an alert, but not a full report, within 72-hours of the credit union reasonably believing a breach occurred.
- The Association, however, urges the Board to clarify that the 72-hour period begins when a credit union “discovers” an intrusion that caused a “material” disruption to credit union activities that the credit union reasonably believes qualifies as a reportable cyber incident.
- We also strongly urge the Board only to require credit unions to report to NCUA a breach of a third-party service provider when the credit union has received a notification from that third-party that the credit union’s sensitive information has been materially compromised. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA) should require these third parties to notify credit unions if such breaches occur. Without receiving a notification from the third-party, credit unions have no reliable way to know whether the third-party has experienced a cyber incident.

## The Association's Detailed Comments

The Association supports the Board's proposal to update its Part 748 rules so that federally-insured credit unions experiencing a cyber intrusion by hackers must provide NCUA with an early alert, but not a full report, within 72-hours. We urge the Board, however, to clarify that the 72-hour period begins when the credit union "discovers" a breach that causes a "material" disruption to credit union activities. In addition, credit unions should only be required to report a breach at a third-party service provider to NCUA if the third party has notified the credit union of the breach.

Since Part 748 already requires credit unions to notify members if their personal information has been breached, the Association believes that this proposal, once finalized, should be compliant with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) that President Biden signed into law in March 2022. Once the Cybersecurity and Infrastructure Security Agency (CISA) issues its guidance on CIRCIA, we encourage the Board to limit regulatory burdens on credit unions by issuing its own guidance clarifying that NCUA examiners will treat following Part 748 as a CIRCIA-compliance safe harbor.

The Association urges the Board to clarify in the final rule that the 72-hour reporting period begins once a credit union "discovers" what it reasonably believes to be a cyber incident. A cyber intrusion may not be discovered for some time. While we believe that it is the Board's intention for credit unions only to be required to report incidents that they have actually discovered, the text of the proposal is unclear regarding situations where a credit union experiences events that could later be cast as the credit union's staff unreasonably believing that a cyber incident has not occurred when in fact it had. Since potential second guessing creates compliance burdens in the form of regulatory uncertainty, we urge the Board to clarify that the credit union must in fact discover a cyber incident before it is required to report it.

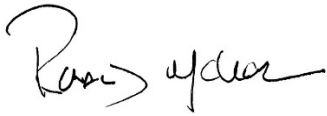
We also urge the Board to revise the definition of a "reportable cyber incident" to require a "material" disruption of business operations in order for a credit union to be required to alert to NCUA. Including minor, non-material cyber incidents in the reporting process could create excessive paperwork burdens on credit unions that would provide NCUA with information of limited usefulness. In addition, we are concerned that NCUA receiving too much information about non-material cyber incidents would strain the agency's resources and/or create a "needle in a haystack" scenario where reports of serious cyber incidents could go unnoticed at first because they are crowded out by reports of non-material incidents.

Regarding breaches of third-party service providers, we strongly urge the Board only to require credit unions to report to NCUA a service provider's cyber incident if the third party has reported the breach to the credit union because it involved the credit union's sensitive data subject to the Part 748 rules. CIRCIA should require these third parties to notify the credit union when such a breach occurs. Requiring credit unions also to report possible breaches at a third-party that it "reasonably believes" occurred is not workable in practice because that would require credit unions to guess at what might be going in computer systems that are not under its own control.

The final rule should reflect the reality that credit unions can only reasonably know that a breach has occurred at a third party if the third party notifies the credit union, as CIRCIA now requires.

The Association appreciates the opportunity to comment on the NCUA's proposed rule on Cyber Incident Notification Requirements for Federally Insured Credit Unions. If you have any questions about our comments or require further information, please do not hesitate to contact the Association at [govaff-reg@ccua.org](mailto:govaff-reg@ccua.org).

Sincerely,

A handwritten signature in black ink, appearing to read "Ronald McLean". The signature is fluid and cursive, with a large initial "R" and a long horizontal stroke at the end.

Ronald McLean  
President/CEO  
Cooperative Credit Union Association, Inc.  
[rmclean@ccua.org](mailto:rmclean@ccua.org)