How Credit Unions Can Prepare For 3-Day Cyber Report Rule

By **Alexander Boyd and Colin Black** (March 27, 2023)

Alexander Boyd

Colin Black

On Feb. 16, the National Credit Union Administration unanimously approved a final rule that requires federally insured credit unions to report "reportable cyber incidents" to the NCUA as soon as possible, and in no event later than 72 hours after the credit union reasonably believes that it has experienced a reportable cyber incident.[1] The final rule becomes effective on Sept. 1.

With this new rule and the NCUA's focus on cybersecurity in its 2023 supervisory priorities,[2] the NCUA continues to expand its role in safeguarding member data and holding federally insured credit unions to high cybersecurity and data privacy standards.

The broad 72-hour rule applies to both disruptive incidents like ransomware or network outages and to privacy incidents involving unauthorized access to a wide range of member information, whether occurring at the credit union or a service provider.

With a quick notice requirement, credit unions must prepare well in advance of an incident to ensure they can comply with the rule while also responding to the operational challenges associated with a data security incident. The rule also adds a new layer to the obligations faced by credit unions under existing NCUA guidance and state data breach notification laws.

Through an effective incident response plan, data management and vendor due diligence, credit unions can ensure compliance with the new rule and increase their own cybersecurity posture.

Existing Incident Reporting Guidance

In 2005, the NCUA first issued data incident reporting guidelines interpreting Section 501(b) of the Gramm-Leach-Bliley Act: the Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice.[3]

Under the guidance and the NCUA's 2006 legal opinion discussing the guidance,[4] federally insured credit unions are required to notify potentially involved members, 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 unauthorized access to "sensitive member information" and misuse has occurred or is reasonably possible.

The guidance also advises credit unions to notify law enforcement about incidents involving federal criminal violations. These existing requirements under the guidance will continue to apply even when the new 72-hour reporting rule goes into effect, as the scope of the two requirements are not identical.

Updated Incident Reporting Requirements

Under the new rule, a federally insured credit union must notify their NCUA designated point of contact of the occurrence of a reportable cyber incident as soon as possible but no later than 72 hours after the credit union reasonably believes that it has experienced a reportable cyber incident or within 72 hours of being notified by a third party of such an incident.

The NCUA anticipates providing specific guidance on the reporting logistics before the rule's effective date.

A cyber incident[5] becomes a "reportable cyber incident" if it leads to one or more of the following:

- "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"; 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, or other third-party data hosting provider or by a supply chain compromise."[6]

Unlike the 36-hour cyber incident reporting rule adopted by federal banking regulators in 2022 that focuses on operational disruptions — for example, that may arise from ransomware or other disruptive cyberattacks[7] — the NCUA rule also requires prompt notice of certain incidents that affect the confidentiality of member or credit union information.

The NCUA explained that if a credit union "becomes aware that a substantial level of sensitive data is unlawfully accessed, modified, or destroyed, or if the integrity of a network or member information system is compromised, the cyber incident is reportable."[8]

The rule broadly defines covered "sensitive data" to mean "any information which, by itself or in combination with other information, could be used to cause harm to a credit union or credit union member and any information concerning a person or their account which is not public information, including any non-public personally identifiable information."[9]

This definition is significantly broader than the operative definition of sensitive member information used in the existing guidance.

While the rule includes very broad definitions, it also includes important qualifiers. As explained in the preamble to the new rule, the NCUA was intentional in its use of the substantial qualifier.

The NCUA should be notified of cyber incidents that "are extensive or significant to the [credit union] or its members (or both), rather than minor or inconsequential."[10] This will be a fact-specific inquiry based on the circumstances of each incident and how it affects the specific impacted credit union and its members.

The new rule, which primarily amends Title 12 of the Code of Federal Regulations, Section 748.1, is supplemental to, and not in lieu of, the guidance found in Appendix B to Part 748. Accordingly, a federally insured credit union will soon be subject to both the guidance and the new 72-hour reporting rule.

Practical Guidance for Credit Unions

With the new rule becoming effective on Sept. 1, credit unions should begin preparations now to ensure they can comply with the new rule when responding to an already challenging cyber incident.

First, every federally insured credit union, irrespective of charter status, should ensure that its data incident response plan is consistent with the new rule. At a minimum, this should include the following points:

- Quickly identifying and escalating potential "reportable cyber incidents" during the initial phases of an incident response to ensure prompt notice to the NCUA when required;

- Establishing criteria or guidance for determining the point at which a cyber incident becomes a substantial cyber incident based on the credit union's specific characteristics;

- Identifying the individual(s) who will be responsible for determining whether an incident has become a reportable cyber incident;

- Ensuring consistency between the credit union's obligations under the new rule, the existing guidance, state law, and under other separate contractual requirements;

- Documenting the logistics for the NCUA notice, including the content of that notice, the recipient of the notice, and the method of providing and documenting the notice;

- Establishing a procedure for documenting both notifications to the NCUA and determinations not to notify the NCUA; and

- Preparing approved form notices that can be readily adapted in the event of a cyberattack.

The incident response plan should be distributed to all individuals who may be required to carry out the plan and should be retained in both physical and digital formats to ensure availability in the event of a cyberattack.

Once adopted, the credit union should periodically practice its new incident response plan to identify any gaps and to increase the effectiveness of the credit union's response.

Credit unions should take stock of their sensitive data, where that data is stored — including with any service providers — and how long it is retained.

These types of data flow diagrams and sensitive information audits can reduce the scope of an incident by minimizing the amount and locations of sensitive information. Understanding where sensitive data resides is also an important first step in knowing whether sensitive data may be involved in a cyber incident.

Finally, credit unions should assess their existing service provider relationships and agreements to confirm compliance with the updated rule. Vendor agreements should contain specific notification obligations that cover sensitive data, including sensitive member information, and provide the credit union with sufficient information to evaluate its notice obligations under the new rule.

Even service providers that do not have access to member information but that may provide certain infrastructural services are within the scope of the new rule.

Alexander D. Boyd is a shareholder and Colin H. Black is an associate at Polsinelli PC.

[1] NCUA Newsroom, NCUA Board Approves Final Rule on Cyber Incident Reporting Requirements (Feb. 16, 2023); https://ncua.gov/files/agenda-items/cyber-incident-notification-requirements-final-rule-20230216.pdf.

[2]https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/ncuas-2023-supervisory-priorities.

[3] 12 C.F.R. Part 748, App. B.

[4] NCUA Legal Opinion 06-0332.

[5] "Cyber incident means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information

system." 12 CFR § 748.1(c)(2), as amended September 1, 2023.

[6] 12 CFR § 748.1(c)(1), as amended September 1, 2023.

[7] https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

[8] Preamble, https://ncua.gov/files/agenda-items/cyber-incident-notification-requirements-final-rule-20230216.pdf.

[9] 12 CFR § 748.1(c)(2), as amended September 1, 2023.

[10] Preamble, https://ncua.gov/files/agenda-items/cyber-incident-notification-requirements-final-rule-20230216.pdf.