Cyber Incident Notification Requirements

NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: August 2023 **LETTER NO: 23-CU-07**

TO: Federally Insured Credit Unions

SUBJ: Cyber Incident Notification Requirements

ENCL:
- Cyber Incident Reporting Quick Reference Guide
- NCUA Secure Email Message Center Instructions

Dear Boards of Directors and Chief Executive Officers:

Beginning on September 1, 2023, all federally insured credit unions must notify the NCUA as soon as possible, and no later than 72 hours, after the credit union reasonably believes it has experienced a reportable cyber incident or received a notification from a third party regarding a reportable cyber incident.

This letter summarizes the amendments to part 748, known as the Cyber Incident Notification Requirements rule. It also provides instructions on what and how to report to the NCUA, and includes examples of both reportable (see Appendix A) and non-reportable (see Appendix B) incidents.[1] To facilitate incident reporting, the NCUA is also enclosing a cyber incident reporting quick reference guide.

Summary

The Cyber Incident Notification Requirements rule defines a cyber incident as 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.

The rule then defines a reportable cyber incident as any substantial cyber incident that leads to one or more of the following outcomes:

- *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.

This first prong of the reportable cyber incident definition requires a federally insured credit union to report a cyber incident that leads to a substantial loss of confidentiality, integrity, or availability of a member information system as a result of the exposure of sensitive data, disruption of vital member services, or has a serious impact on the safety and resiliency of operational systems and processes. For example, if a federally insured credit union becomes aware that 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. If the credit union becomes aware that a member information system has been unlawfully modified or sensitive data has been left exposed to an unauthorized person, process, or device, that cyber incident is also reportable.

There may be incidents that do not trigger reporting under the amended regulation but involve unauthorized access to or use of sensitive member information. In such cases, credit unions can continue to rely on the framework in Appendix B to part 748, which includes notifying the appropriate NCUA regional director. Appendix B also reflects the NCUA's interpretation of the Gramm-Leach-Bliley Act's security program requirement, which includes notifying its members of a security incident involving the unauthorized access or use of the member's information.

- *A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.*

  The second prong of the reportable cyber incident definition requires reporting to the NCUA when a cyberattack disrupts business operations, vital member services, or a member information system. For example, a distributed denial of service (DDoS) attack that disrupts member account access leading to substantial system outages is reportable under this prong. However, cyber events such as blocked phishing attempts, failed attempts to gain access to systems, or unsuccessful malware attacks would not be reportable.

  There are many technical reasons why services may not be available at any given time: for example, computer servers are offline for maintenance or systems are being updated. Such events are routine and thus would not be reportable to the NCUA. However, an unexpected malfunction that disrupts member account access for a significant period would be reportable under this prong.

- *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 third prong of the reportable cyber incident definition requires a federally insured credit union to notify the agency either when a third-party service provider informs the credit union that the credit union's sensitive data or business operations have been compromised or disrupted as a result of a cyber incident experienced by the third-party service provider or upon the credit union forming a reasonable belief this has occurred, whichever occurs sooner.
>
> A reportable cyber incident does not include any event where the cyber incident is performed in good faith by an entity in response to a specific request by the owner or operators of the system. Contracting a third party to conduct a penetration test is an example of an incident that would be excluded from reporting.

The overall definition of a reportable cyber incident is intended to capture the reporting of substantial cyber incidents. A credit union's determination of "substantial" depends on a variety of factors, including the size of the credit union, the type and impact of the loss, and its duration. The NCUA expects a federally insured credit union to exercise reasonable judgment in determining whether it experienced a substantial cyber incident that is reportable to the agency. If a federally insured credit union is unsure as to whether a cyber incident is reportable, it should contact the NCUA as soon as possible.

Notification Framework

Timeframe

The rule requires a federally insured credit union that experiences a reportable cyber incident to report the incident to the NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes that it experienced a reportable cyber incident. The 72 hours begins when the credit union forms a reasonable belief a reportable cyber incident has taken place.

When a federally insured credit union receives a notification from a third party that sensitive data has been compromised or business operations have been disrupted due to a cyber incident, the credit union has 72 hours to report to the NCUA. This timeframe starts from the moment the credit union receives the notification from the third party or when the credit union forms a reasonable belief that such an incident has occurred, whichever is sooner.

How to Report

To report a cyber incident, federally insured credit unions may notify the NCUA through one of the following channels:

- Call the NCUA at 1.833.CYBERCU (1.833.292.3728) and leave a voicemail; or

- Use the National Credit Union Administration Secure Email Message Center to send a secure email to cybercu@ncua.gov.[2]

What to Report

Federally insured credit unions should be prepared to provide as much of the following information as is known at the time of reporting:

- Credit union name;
- Credit union charter number;
- Name and title of individual reporting the incident;
- Telephone number and email address;
- When the credit union reasonably believed a reportable cyber incident took place; and
- A basic description of the reportable cyber incident, including what functions were, or are reasonably believed to have been affected or if sensitive information was compromised.

At the time of initial notification, do not send the NCUA:

- Sensitive personally identifiable information;
- Indicators of compromise;
- Specific vulnerabilities; or
- Email attachments.

What to Expect

If the NCUA requires additional information or clarification, the NCUA will follow up with the credit union directly.

Implementation Guidelines

Credit unions should complete the following steps when implementing the rule.

Update Response Plan

Review the existing incident response plan and update it to align with the new rule. This includes incorporating the reporting requirement timeframes and procedures for notifying the NCUA. Ensure the plan includes clear guidelines for identifying reportable incidents and escalation procedures for notifying management and the NCUA.

Review Contracts

Review contracts with critical service providers to determine if there are provisions requiring timely notification of cyber incidents.

Train Employees

Provide training to all employees, emphasizing the importance of reporting cyber incidents and the potential consequences of noncompliance. Ensure that employees understand their role in identifying and reporting incidents and provide them with necessary resources and guidance.

Monitor and Review

Regularly monitor and review the cyber incident reporting process to validate its effectiveness. Conduct periodic tests and exercises to evaluate the efficiency of the incident response plan and reporting procedures. Use lessons learned from these exercises to make improvements and update the plan.

Document All Incidents

Document all cyber incidents, regardless of whether they meet the reporting criteria, and maintain records in accordance with the organization's retention policies. This documentation is essential and serves as a valuable resource for future incident response and reporting efforts. Documentation also provides an audit trail to support management's reporting decisions.

Specifically, document:

- Indicators of compromise;
- Network information or traffic regarding the attack;
- The attack vector;
- Information on any exfiltrated data; and
- Any forensic or other reports about the reportable cyber incident.

Conclusion

By following these guidelines and implementing the cyber incident notification requirements, your credit union can enhance its overall cybersecurity posture and improve incident response capabilities.

Credit unions should maintain open communications with the NCUA regarding any questions or concerns about the new rule. Credit unions may also utilize the NCUA's Cybersecurity Resources webpage to stay informed on guidance, best practices, and industry trends in cybersecurity.

Sincerely,

/s/

Todd M. Harper
Chairman

---

[1] This guidance only pertains to reporting under this cyber incident notification rule. The credit union should also be aware of other state or federal reporting requirements.

[2] To ensure receipt of your secure message you must use the National Credit Union Administration Secure Email Message Center to send the email. See enclosure NCUA Secure Email Message Center Instructions.

Last modified on 08/14/23