# *DCU BULLETIN*

***Division of Credit Unions***
***Washington State Department of Financial Institutions***


***Phone: (360) 902-8701*** ***FAX: (360) 704-6909***



May 16, 2024 No. B-24-03


# Updated Guidance on Cyber Incidents and Data Security Breach Notification

## Introduction

This bulletin offers details on recently enacted regulation changes, along with regulatory guidance. This bulletin summarizes state and federal notification requirements when a credit union has a cyber incident and/or unauthorized access to sensitive information. This information aims to assist in establishing a security response system to effectively address cyber incidents, incidents of security breaches, and notification to appropriate stakeholders. Credit unions should ensure their incident response program includes plans and procedures for both cyber incident reporting and data breach notifications.

Cyber incidents and unauthorized access to members' personal information[1] could potentially occur, despite the measures credit unions have implemented to safeguard information technology systems against security incidents and both internal and external breaches. Typically, these measures involve ensuring that third-party service providers are securing members' personal information, conducting thorough testing of your credit union's systems (including external and internal penetration testing), and taking other crucial steps to reduce the risk of a security breach.

### New NCUA Regulation on Incident Reporting

An amendment to part 748.1, known as the Cyber Incident Notification Requirements rule, took effect 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.

[1] "Personal information" is defined in Chapter 19.255 RCW.

Credit unions must update their incident response program to align with the new rule. Although the rule became effective several months ago, examiners are finding some credit unions have not updated their programs, policies, and procedures to incorporate the rule or they have updated them incorrectly. In a few instances, credit unions removed provisions about reporting breaches, which have separate requirements beyond reporting the initial incident. The program should incorporate the reporting requirement timeframes and document procedures for notifying the NCUA of a significant cyber incident. The NCUA has covered the new regulation in their Letter to Credit Unions 23-CU-07.

The letter summarizes the amendment and specifies how to report a cyber incident, what to report, the timeframe, and what to expect going forward. The letter included five steps to take in implementing the rule. Notification should focus on basic details of a cyber incident and should not include sensitive personally identifiable information. Reporting to the NCUA is the credit union's duty. Even if a cyber incident occurred with a third party, it is the credit union that must report the incident.

## Other Existing Regulations and Laws about Data Breach Notification

In addition to the new rule, credit unions must comply with both regulation 12 CFR 748 Appendix B and RCW 19.255.010.

12 CFR 748 Appendix B provides guidance on response programs for unauthorized access to member information and member notice. It outlines the security guidelines, risk assessment and controls, and responsibilities regarding service providers. Further, it provides guidance on implementing a risk-based response program to address incidents of unauthorized access to member information and specifies the components of a response program and member notice.

RCW 19.255.010 requires institutions to disclose any breach of security to affected residents, mandates prompt notification and outlines specific requirements for the content and timing of such notifications. If a breach affects more than 500 Washington residents, the Attorney General must be notified within 30 days of the discovery of the breach. The notification must include details about the breach and steps taken to contain it. 12 CFR 748 may not agree perfectly with the RCW. Credit unions will need to carefully evaluate both regulations to ensure compliance with both.

## Response Program Needed

The impact of a security breach incident presents risks if the credit union is not ready to respond quickly with a well-thought-out plan. Response programs need to be in place before an event of security incident or a breach occurs.

A response program should include plans and procedures following cyber incident reporting and data breach notification processes. By prioritizing compliance with these regulations and maintaining a robust incident response program, credit unions can mitigate the risks associated with data breaches and safeguard the trust of their members.

If you have any questions about this bulletin or would like more information, please contact the Division of Credit Unions at dcu@dfi.wa.gov or (360) 902-8701.