U.S. Risk, LLC

NEWS ALERT

Effective September 1, 2023: Federally insured credit unions will be required to report a data breach within 72 hours to the National Credit Union Administration (NCUA) Board.

CYBERSECURITY: CREDIT UNIONS HAVE NEW 72 HOUR REPORTING RULE

Credit unions will need to quickly update their data incident response teams policies and procedures to meet the September 1st effective date for this new cybersecurity reporting rule.

A "reportable" cyber incident, as defined in the new rule, is an incident that leads to at least one of the following outcomes. If a credit union experiences any of these, it must notify the NCUA "as soon as possible but no later than 72 hours" from the time it reasonably believes that it has experienced a reportable cyber incident.

- A "substantial loss" of the confidentiality, integrity, or availability of a network or member information system that causes the unauthorized access to or exposure of "sensitive data," disrupts vital member services, or seriously impacts 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.
- 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.

› Examples of Reportable Incidents

The NCUA has indicated it will issue additional guidance before September 1st, including examples of both non-reportable and reportable incidents and how notice must be provided. Currently reportable cyber incidents include:

- 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
- If a credit union becomes aware that a member information system has been unlawfully modified and/or sensitive data has been left exposed to an unauthorized person, process, or device, regardless of intent
- A DDoS attack that disrupts member account access
- A computer hacking incident that disables a credit union's operations
- A ransom malware attack that encrypts a core banking system or backup data
- Third-party notification to a credit union that they have experienced a breach of a credit union employee's personally identifiable information
- A detected, unauthorized intrusion into a network information system
- Discovery or identification of zero-day in a network or information system
- Internal breach or data theft by an insider
- Member information compromised as a result of card skimming at a credit union's ATM
- Sensitive data exfiltrated outside of the credit union or a contracted third party in an unauthorized manner, such as through a flash drive or online storage account.

Blocked phishing attempts, failed attempts to gain access to systems and unsuccessful malware attempts would not trigger a reporting requirement.

Credit unions should immediately review their data security monitoring and incident response procedures, making sure systems are in place to detect and report cyber incidents within the new timeframe.