Cullen | Dykman

National Credit Union Administration Approves Final Rule on Cyber Incident Reporting Requirements

February 23, 2023

The National Credit Union Administration ("NCUA") Board approved a final rule on cyber incident reporting requirements ("Final Rule"). The Final Rule requires a federally insured credit union ("FICU") to notify the NCUA as soon as possible, but no later than 72 hours, after it reasonably believes a reportable cyber incident has occurred.

Please note that the 72-hour notification requirement provides an early alert to the NCUA and does not require credit unions to provide a full incident assessment to the NCUA within the 72-hour timeframe.

The effective date of the Final Rule is September 1, 2023.

I. Final Rule

Reportable Cyber Incident

The Final Rule defines "reportable cyber incident" as any substantial cyber incident[1] that leads to one or more of the following:

- 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 that has a serious impact on the safety and resiliency of operational systems and processes. Routine events like computer servers being offline and/or systems being updated are not required to be reported to the NCUA.
- A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities. Blocked phishing attempts, failed attempts to gain access to systems, or unsuccessful malware attacks do not need to be reported.
- 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.

Please note that there is no notification requirement for an incident occurring at any third-party that, unbeknownst and unrelated to the FICU, holds information about the FICU's members or employees. Additionally, a FICU will not be required to report an incident performed in good faith by an entity in response to a request by the owner or operator of the information system. An example of an incident excluded from reporting would be

the contracting of a third-party to conduct a penetration test.

Reporting Timeframe

The Final Rule requires a FICU to notify the NCUA as soon as possible but no later than 72 hours after the FICU reasonably believes that a reportable cyber incident has occurred.

Reporting Process

The NCUA will determine the necessity and frequency of follow-up communications on a case-by-case basis. The NCUA is aware that during a reportable cyber incident, FICUs will be focused on recovery and, thus, the agency will generally limit contact during such incidents to minimize the burden on FICUs.

Third-Party Compromise

The Final Rule does not impact existing contractual relationships. There is no requirement that FICUs amend existing contracts to comply with the Final Rule.

II. New York State Reporting Requirements

Please note that FICUs operating or having members in New York may also be subject to certain New York State cyber reporting requirements. These requirements are discussed below.

Part 500

The New York Department of Financial Services ("NYDFS") has a Cybersecurity Regulation ("Part 500") requiring a covered entity[2] to report data breaches within 72 hours of their discovery.

Part 500.17(a)(1) of NYDFS's Cybersecurity Regulation specifically requires notice, within 72 hours of determining there has been a cybersecurity event, when the event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity or when notices are required to be provided to any government body, self-regulatory agency or any other supervisory body.

Part 500 also requires that covered entities submit a written statement to the NYDFS each year to certify that they have complied with this rule. Covered entities must also maintain all records, schedules and data supporting this certificate for a period of five years.

NY GBL Section 899-aa

Section 899-aa of the New York General Business Law requires certain disclosures in the event of unauthorized access to or acquisition of computerized data that compromises the security, confidentiality or integrity of private information of a New York resident.

Under Section 899-aa, any person or business which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the

breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. In the event a New York resident is to be notified under Section 899-aa, the state Attorney General, the Department of State and the Division of State Police must also be notified as to the timing, content and distribution of the notices and approximate number of affected persons. A copy of the template of the notice sent to affected persons is also required to be provided.

III. Conclusion

Given the growing frequency and severity of cyber incidents within the financial services industry, it is important that FICUs understand and comply with the requirements set forth in the Final Rule and be aware of the New York reporting requirements that may apply.

The NCUA will be providing further supervisory guidance prior to the effective date of the Final Rule. However, cyber incidents may still be reviewed during an annual examination or as part of a supervision contact. This rule does not change the examination and supervision process.

This advisory is a general overview of the Final Rule and is not intended as legal advice. The Final Rule is detailed and must be reviewed in its totality.

If you have any questions about reporting cyber incidents, please feel free to contact Joseph D. Simon at (516) 357-3710 or via email at jsimon@cullenllp.com, Kevin Patterson at (516) 296-9196 or via email at kpatterson@cullenllp.com, Elizabeth A. Murphy at (516) 296-9154, or via email at emurphy@cullenllp.com, or Gabriela Morales at (516) 357-3850 or via email at gmorales@cullenllp.com.

Footnotes

[1] 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.

[2] Covered Entity means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

Practices

- Banking and Financial Services
- Regulatory and Compliance

Attorneys

- Joseph D. Simon
- Kevin Patterson

- Elizabeth A. Murphy
- Gabriela Morales