This document is scheduled to be published in the Federal Register on 03/01/2023 and available online at **federalregister.gov/d/2023-03682**, and on **govinfo.gov**

7535-01-U

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

RIN 3133-AF47

Cyber Incident Notification Requirements for Federally Insured Credit Unions

AGENCY: National Credit Union Administration.

ACTION: Final rule.

SUMMARY: The National Credit Union Administration (NCUA or agency) is amending Part 748 of its regulations to require a federally insured credit union (FICU) 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 FICU reasonably believes that it has experienced a reportable cyber incident. This notification requirement provides an early alert to the NCUA and does not require a FICU to provide a detailed incident assessment to the NCUA within the 72-hour time frame.

DATES: The effective date of this final rule is September 1, 2023.

FOR FURTHER INFORMATION CONTACT: *Policy*: Christina Saari, Information Systems Officer, Office of Examination and Insurance, at (703) 283-0121; *Legal:* Gira Bose, Senior Staff Attorney, Office of General Counsel, at (703) 518-6540.

SUPPLEMENTARY INFORMATION:

I. Introduction

A. Background

The NCUA's requirement that FICUs develop written security programs and report certain activity to the NCUA is codified in 12 CFR part 748. In July 2022, the NCUA Board

(Board) approved a notice of proposed rulemaking (proposal or proposed rule) that would require a FICU to notify the NCUA of any cyber incident that rises to the level of a reportable cyber incident.[1] The proposed rule would require such notification as soon as possible but no later than 72 hours after a FICU reasonably believes that a reportable cyber incident has occurred.

As stated in the proposed rule, given the growing frequency and severity of cyber incidents within the financial services industry, it is important that the NCUA receive timely notice of cyber incidents that disrupt a FICU's operations, lead to unauthorized access to sensitive data, or disrupt members' access to accounts or services.

B. Summary of Proposed Rule

The proposed rule added a provision to 12 CFR 748.1 for the NCUA to require notification of any *cyber incident* that rises to the level of a *reportable cyber incident* as soon as possible but no later than 72 hours after a FICU reasonably believes that a *reportable cyber incident* has occurred. As first stated in the proposed rule and finalized here, in accordance with § 704.1(a) of the NCUA's regulations, this rule also applies to federally chartered corporate credit unions and federally insured, state-chartered corporate credit unions.

The proposed rule defined 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.[2]

---

[1] 87 FR 45029 (July 27, 2022).
[2] 6 U.S.C. 659(a)(5).

The proposed rule defined a *reportable cyber incident* as any substantial cyber incident that leads to one or more of the following: a substantial loss of confidentiality,[3] integrity,[4] or availability of a network or member information system[5] that results from the unauthorized access to or exposure of sensitive data,[6] disrupts[7] vital member services,[8] 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[9] or exploitation of vulnerabilities; and/or a disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise[10] of a credit union service organization, cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

The proposed rule definition excluded any event where the cyber incident was performed in good faith by an entity in response to a specific request by the owner or operator of the information system.

---

[3] *Confidentiality* means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. *See* https://csrc.nist.gov/glossary/term/confidentiality. The agency is using definitions from the National Institute of Standards and Technology (NIST), as appropriate. NIST is a familiar and trusted source in the cybersecurity arena and is routinely cited by the Federal Financial Institutions Examination Council and individual federal agencies.

[4] *Integrity* means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. *See* https://csrc.nist.gov/glossary/term/integrity.

[5] *Member information system* means any method used to access, collect, store, use, transmit, protect, or dispose of member information. 12 CFR part 748, appendix A, section I.B.2.e.

[6] *Sensitive data* is defined as 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 the person's account which is not public information, including any non-public personally identifiable information.

[7] A *disruption* is an unplanned event that causes an information system to be inoperable for a length of time. https://csrc.nist.gov/glossary/term/disruption.

[8] *Vital member services* means informational account inquiries, share withdrawals and deposits, and loan payments and disbursements. 12 CFR 749.1

[9] *Cyberattack* is an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. *See https://csrc.nist.gov/glossary/term/Cyber_Attack#:~:text=An%20attack%2C%20via%20cyberspace%2C%20targeting%20an%20enterprise%E2%80%99s%20use,SP%201800-10B%20from%20NIST%20SP%20800-30%20Rev.%201*.

[10] A *compromise* is the unauthorized disclosure, modification, substitution, or use of sensitive data or the unauthorized modification of a security-related system, device, or process in order to gain unauthorized access. *See https://csrc.nist.gov/glossary/term/compromise#:~:text=Definition(s)%3A,an%20object%20may%20have%20occurred*.

The Board is adopting this final rule largely as proposed to give the NCUA early notice of substantial cyber incidents that have consequences for FICUs as stated in the rule.

Shortly before the Board issued its proposed rule, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Cyber Incident Reporting Act) requiring covered entities to report covered cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) not later than 72 hours after the entity reasonably believes that a covered cyber incident has occurred.[11] CISA has until 2025 to publish a final rule implementing the Cyber Incident Reporting Act's requirements, including defining the terms used therein. Nevertheless, as stated in the proposed rule, the Board believes that it would be imprudent in light of the increasing frequency and severity of cyber incidents to postpone a notification requirement until after CISA promulgates a final rule. To the extent possible, and as appropriate for the credit union system, this final rule uses terminology and a reporting framework that Congress outlined in the Cyber Incident Reporting Act. The Board believes it is in the best interest of the credit union system to align the NCUA's rule with the Cyber Incident Reporting Act to provide uniform and timely cyber incident reporting. It is the intention of the Board for the NCUA to coordinate with CISA on any future credit union cyber incident reporting to avoid duplicate reporting to both the NCUA and CISA.

II. Overview of the Final Rule

After carefully considering the comments received, the NCUA is issuing this final rule largely as proposed, as discussed in this section of the preamble.

Definitions

The proposed rule defined a *reportable cyber incident* as, among other things, any substantial cyber incident that leads to a *substantial* loss of confidentiality, integrity, or

---

[11] The Cyber Incident Reporting for Critical Infrastructure Act of 2022, part of the Consolidated Appropriations Act of 2022, Division Y, Pub. L. 117–103 (Mar. 15, 2022), is available at *https://www.congress.gov/bill/117th-congress/house-bill/2471/text*.

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. Some commenters felt that the duplicate use of the term *substantial* was redundant. That was the not the intent of the definition. While the word used is the same, *substantial* applies in two different contexts and thus is retained in both places to ensure that the agency receives notification of cyber incidents that are substantial. This terminology also aligns with the language used in the Cyber Incident Reporting Act. In the event such a cyber incident is one that leads to a *substantial* loss of confidentiality, integrity, or availability of a network or member information system, as opposed to a minimal loss, then such incident would be reportable to the agency.

The first prong of the *reportable cyber incident* definition will require a FICU to notify the NCUA of 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 that has a serious impact on the safety and resiliency of operational systems and processes. For example, if a FICU 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. If the 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, that cyber incident is also reportable, irrespective of intent.

There are many technological reasons why services may not be available at any given time as, for example, computer servers are offline, or systems are being updated. Such events are routine and thus would not be reportable to the NCUA. However, a failed system upgrade or change that results in unplanned widespread user outages for FICU members and employees would be reportable.

The second prong of the *reportable cyber incident* definition will require reporting to the NCUA in the event of a cyberattack that leads to a disruption of business operations, vital member services, or a member information system. Cyberattacks that cause disruption to a FICU's business operations, vital member services, or a member information system must be reported to the NCUA within 72 hours of a FICU's reasonable belief that it has experienced a cyberattack. For example, a distributed denial of service (DDoS) attack that disrupts member account access will be reportable under this prong.

Blocked phishing attempts, failed attempts to gain access to systems, or unsuccessful malware attacks do not have to be reported.

The third prong of the *reportable cyber incident* definition will require a FICU to notify the agency within 72 hours after a third-party has informed a FICU that the FICU's sensitive data or business operations have been compromised or disrupted as a result of a cyber incident experienced by the third-party or upon the FICU forming a reasonable belief this has occurred, whichever occurs sooner. A cyber incident, under the third prong would also only be reportable in the event that the third-party has a relationship with the FICU. The rule does not impose a notification requirement on a FICU for an incident occurring at any third-party that, unbeknownst and unrelated to the FICU, holds information about individuals who happen to be FICU members or employees.

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.[12]

[12] A penetration test is a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system. See Assessing Security and Privacy Controls in Information Systems and Organizations, NIST Special Publication 800-53A Revision 5 at 697. Available at *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar5.pdf*.

III. Legal Authority

The Board issues this final rule pursuant to its authority under the Federal Credit Union Act (FCUA). Section 209 of the FCUA is a plenary grant of regulatory authority to the Board to issue rules and regulations necessary or appropriate to carry out its role as share insurer for all FICUs.[13] Section 206 of the FCUA requires the agency to impose corrective measures whenever, in the opinion of the Board, any FICU is engaged in or has engaged in unsafe or unsound practices in conducting its business.[14] Accordingly, the FCUA grants the Board broad rulemaking authority to ensure that the credit union industry and the National Credit Union Share Insurance Fund (Share Insurance Fund) remain safe and sound.

IV. Discussion of Public Comments Received on the Proposed Rule

The proposed rule provided for a 60-day public comment period, which closed on September 26, 2022. The NCUA received 17 comments in response to the proposed rule. These comments came from credit unions, credit union trade associations and leagues, service providers, and individual members of the public.

Twelve commenters expressed support for the proposal. One commenter felt it was premature for the Board to issue a rule at this time because promulgating a rule now could lead to conflicts with standards yet to be determined by CISA, which Congress has tasked with issuing cybersecurity notification rules across many sectors, including financial services.

Four credit union commenters disagreed with the premise that knowing about and responding to cyber incidents is important to the NCUA's mission. These commenters stated that the preamble articulated no benefits to members and that members are already protected by a FICU's data security program, which the NCUA has the opportunity to evaluate during the examination cycle. These four commenters stated that the NCUA should show deference to a

---

[13] 12 U.S.C. 1789(a)(11).

[14] 12 U.S.C. 1786(b)(1). There are a number of references to "safety and soundness" in the FCUA. See 12 U.S.C. 1757(5)(A)(vi)(I), 1759(d & f), 1781(c)(2), 1782(a)(6)(B), 1786(b), 1786(e), 1786(f), 1786(g), 1786(k)(2), 1786(r), 1786(s), and 1790d(h).

FICU's decision regarding whether or not to report an incident because the FICU will be in the best position to know whether it has met the elements of a reportable cyber incident.

The Board has considered these comments and has determined to proceed to a final rule at this time. As discussed in the preamble to the proposed rule, the financial services sector is one of the main critical infrastructure sectors targeted by cyberattacks. The agency has a statutory obligation to ensure the safety and soundness of the credit union system and the Share Insurance Fund. Thus, the NCUA must be made aware of cyber incidents that could significantly impact FICUs and their members. Commenters are correct in that this rule does not change the NCUA's ability to review data security programs during the examination cycle. This rule merely requires early notification to the agency of substantial cyber incidents. Early awareness can help the NCUA react to emerging threats to FICUs and the broader financial system before they become systemic. As stated in the proposed rule, this notification requirement is intended to serve as an early alert to the agency and is not intended to include a lengthy assessment of the incident. The NCUA will be providing additional reporting guidance prior to the final rule going into effect. However, anytime a FICU is unsure as to whether a cyber incident is reportable, the Board encourages the FICU to contact the agency.

Commenters focused on the following specific issues:

Reporting Timeframe

The proposed rule put forward a 72-hour reporting window for FICUs to notify the NCUA of a *cyber incident* that rises to the level of a *reportable cyber incident*. The proposal asked commenters to discuss whether 72 hours is appropriate or if another time frame is warranted, such as 36 hours as the Federal banking agencies require. Fourteen commenters expressed support for the 72-hour reporting window. Three of these commenters asked the agency to be aware that, while 72 hours is generally reasonable, even this may be burdensome for smaller institutions. One commenter stated that the proposed timeframe will correspond with additional administrative burden for credit unions. One commenter preferred the 36-hour time

frame since this would be consistent with the Federal banking agencies' rule and should not be burdensome in light of the limited information being sought.

Three commenters recommended that the 72-hour reporting period begin only once a FICU has actually discovered a *reportable cyber incident*, as the Federal banking agencies require, rather than requiring FICUs to come to a reasonable belief that a *reportable cyber incident* has occurred. Another commenter stated that the Board should not require reporting until the FICU is aware of helpful details.

This final rule maintains the reporting period set forth in the proposed rule requiring 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. This is the same reporting requirement CISA must implement under the Cyber Incident Reporting Act. By maintaining the expectation that a FICU does not have a reporting obligation until it has a reasonable belief that a reportable cyber incident has occurred, the Board is providing flexibility based on specific circumstances that may occur. Only once the FICU has formed a reasonable belief that it has experienced a *reportable cyber incident* would the requirement to report within 72 hours be triggered. The Board does not believe this minimal notification requirement would be burdensome to even the smallest institutions. The burden is likely to result from the cyber incident itself. Early notification to the agency could be beneficial in a number of ways, including helping the FICU protect its members and obtaining the agency's guidance with the response.

Reporting Process

With regard to where and how FICUs should report cyber incidents, two commenters stated that they would prefer a single point of contact in the NCUA's central office and multiple methods of reporting – secure online portal, email, and telephone. One commenter expressed a preference for reporting to the regional office but recognized that the NCUA may prefer all FICUs to report to the central office. This commenter suggested that if reporting is done via

portal, then FICUs should be permitted to go back and edit their reporting. Two commenters asked the NCUA to develop a form or checklist that lists the information the agency is looking for. One commenter stated that the NCUA should provide a clear reporting mechanism via secure email or web form. Finally, one commenter expressed support for multiple methods of reporting but suggested that the NCUA permit FICUs to report to their regional office contacts so as to ensure that the NCUA staff evaluating the incident are familiar with the affected FICU's operations.

The proposed rule states that cyber incidents may be reported via email, telephone, or other similar methods that the NCUA may prescribe. The Board believes that this approach addresses the need for flexibility, including if one or more communication channels are impacted by the cyber incident. The NCUA will be providing more detailed reporting guidance before the effective date of the final rule.

One commenter asked for clarity on what follow up communications the agency expects after a FICU provides the initial notification of a reportable cyber incident. The proposed rule stated, "the NCUA anticipates that further follow-up communications between the FICU and the agency will occur through the supervisory process, as necessary," but did not explain what such communications would entail or what the expected frequency or level of detail would be.

The NCUA will determine the necessity and frequency of follow-up communications on a case-by-case basis. Factors in making this determination may include the severity of impact, the ability to recover and restore services, and the potential risk to the financial system. These factors may evolve over time. 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 burden on FICUs.

Confidentiality

Five commenters expressed concern for the security of the information reported to the NCUA and the potential negative consequences to FICUs in the event sensitive information were

to leak. These commenters stated that it is vital for the NCUA to have a secure infrastructure with confidentiality controls and limits on the number of agency personnel with access to the reported information. One commenter asked the NCUA to clarify that cyber incident reports are not only subject to part 792 of the NCUA's rules but are also exempt from Freedom of Information Act (FOIA) requests.

The NCUA receives confidential financial information from FICUs on a routine basis as a function of its role as a financial regulator and insurer. Like all federal agencies, the NCUA must comply with mandatory security standards for federal information and information systems.[15] The NCUA meets these requirements by employing a defense-in-depth[16] approach to information and system security, including robust technical and administrative controls and comprehensive procedures for preventing and addressing potential compromises to information in the NCUA's custody and control.[17]

Reporting under this rule will be subject to part 792 of the NCUA's rules and exempt from FOIA requests under FOIA exemptions 4 and 8, and potentially exemptions 6 and 7(c).[18]

Definition of Reportable Cyber Incident

Eight commenters suggested the NCUA provide more clarity around what the agency considers to be a *substantial* cyber incident. Of these, five commenters stated that the NCUA should focus on the materiality of the incident and include a materiality standard to avoid overreporting and to provide a sufficient threshold to ensure reporting only of major disruptions and not minor ones. One of these commenters stated that the definition of reportable cyber incident itself is acceptable and leaves room to enable ongoing alignment with other frameworks

---

[15] Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. Chapter 35; FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems; FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.

[16] *Defense-in Depth* is the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. *See* https://csrc.nist.gov/glossary/term/defense_in_depth.

[17] NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Federal Information Systems and Organizations.

[18] 12 CFR part 792; 5 U.S.C. 552(b)(4), (6), (7)(c), and (8).

such as future CISA guidance. However, the commenter stated that the definition of *substantial* should include a materiality standard.

One commenter suggested that *substantial* could be defined based on the percentage of members impacted, duration of impact, or other similar metrics which scale with the size of the FICU. Another commenter suggested that any factors used to define *substantial* should be principles-based rather than enumerate different types of data, systems, or other static elements, which can quickly change as best practices and mitigation strategies evolve over time. This commenter noted that, however defined, the agency should grant appropriate deference to the reasonable judgment of the FICU. Another commenter expressed support for the definition of *reportable cyber incident* but stated that rather than just providing a definition of *substantial*, it would be more helpful if the NCUA were to provide examples of reportable incidents.

The Board agrees that a definition that relies on specific data points, systems, or other static elements may be unnecessarily complicated and may quickly become obsolete. By using the term *substantial*, the Board seeks to convey an expectation that the agency will be notified of cyber incidents that are extensive or significant to the FICU or its members (or both), rather than minor or inconsequential. The dictionary definition of *substantial* is "something that is important, essential, considerable in quantity, or significantly great."[19] In lieu of a more complicated definition, the agency intends to add to the examples of reportable cyber incidents provided in the proposed rule. Commenters who requested that a materiality standard be added to the term *substantial* did not offer any definitions or suggest how a *material* cyber incident would be something other than a *substantial* cyber incident. If a FICU is unsure as to whether a cyber incident is reportable, the Board encourages the FICU to contact the agency. However, once the rule is implemented the agency will continue to assess whether further clarity or guidance is needed over time.

---

[19] Merriam Webster Dictionary, available at *https://www.merriam-webster.com/dictionary/substantial*.

Examples of reportable cyber incidents

Three commenters stated that the list of reportable incidents in the proposed rule is helpful and should be kept current. One commenter stated that the NCUA should provide more examples of nonreportable incidents.

The NCUA will be providing additional reporting guidance and examples of reportable incidents and non-reportable incidents prior to the effective date of this final rule. In addition, the NCUA is retaining the examples provided in the proposed rule with some minor edits, as discussed below.

The agency is clarifying the following example which was cited in the proposed rule: "A systems compromise resulting from card skimming," is being changed to "Member information compromised as a result of card skimming at a credit union's ATM."[20]

Third-party compromise

Two commenters noted that contracts with third-party service providers may not perfectly align with the reporting proposed in this rule. One commenter sought clarification that the NCUA is not intending to impact existing contractual relationships. Another commenter stated that FICU reporting of third-party breaches should only be required once the third-party notifies the FICU that its information has been materially compromised. Without receiving information from the third-party, the FICU has no way to know if it has experienced a cyber incident.

One commenter noted that third-parties only provide notification once their investigations are almost complete. Another commenter expressed concerns about the ability of FICUs to make decisions about third-party breaches when third-parties may be reluctant to offer information until they have done their own investigations. Thus, the commenter stated that the NCUA should defer to a FICU's judgment about whether a reportable cyber incident has

[20] See example 7 at 87 FR 45029, 45032 (July 27, 2022).

occurred. Another commenter stated that the NCUA must focus on when the FICU formed a reasonable belief and not when a third-party made that determination. Finally, one commenter stated that the NCUA should not, as suggested by one example in the preamble to the proposed rule, impose a reporting requirement when a FICU employee's personally identifiable information (PII) is implicated in a data breach at another organization that has no affiliation with the FICU.

This rule does not impact existing contractual relationships. While the proposed rule asked FICUs to share how third-parties provide notice to FICUs in the event of a cyber incident, there is no requirement in the proposed or final rules that FICUs amend existing contracts to comply with this rule. The rule requires only that the agency receive notice of a reportable cyber incident that impacts a FICU either within 72 hours of being notified by a third-party or within 72 hours of a FICU forming a reasonable belief that it has experienced a reportable cyber incident. For example, a FICU reasonably may not be aware that a third-party has experienced a *breach* absent a notification from the third-party. However, if a FICU experiences a *disruption* by losing access to its member accounts, it reasonably should be aware that its core service provider has been compromised. The rule does not permit FICUs to provide notice only after the FICU or the third-party have completed all their investigations because the core purpose of the rule is for the agency to receive an early notification that an incident has occurred. The Board recognizes that a FICU's understanding of an incident is likely to evolve, and initial reporting can be incomplete or even inaccurate due to limited information. However, early notification, even if substantively limited, is preferable when compared to delayed notification which may have the effect of impeding the agency's situational awareness.

Finally, regarding the example referenced by one commenter, a substantial cyber incident that leads to the breach of a FICU employee's PII would only be reportable in the event that the third-party has an affiliation or relationship with the FICU by, for example, providing payroll services to the FICU. The example is not intended to impose a notification requirement on a

FICU for an incident occurring at any third-party that, unbeknownst and unrelated to the FICU, holds information about individuals who happen to be FICU members or employees.

Clarification of other sections of Part 748

With regard to catastrophic act reporting under § 748.1(b), two commenters stated that there is insufficient clarity to differentiate this new proposed reporting requirement from the existing catastrophic act reporting requirement and, thus, the latter should be updated to state that it does not include cyber incident reporting. Another commenter stated that, in the event of any overlap between the two reporting requirements, the agency should permit such reporting to receive the longer five-day catastrophic act reporting timeframe.

The Board does not intend to amend the catastrophic act reporting requirement at this time. The Board believes that the two reporting requirements are sufficiently distinct. As stated in the proposed rule, while natural disasters were the leading concern in the aftermath of hurricanes Katrina and Rita, the use of the phrasing "any disaster, natural or otherwise" in the definition of catastrophic act was meant to illustrate other events, such as a power grid failure or physical attack, for example, could have a similar impact on access to member services and vital records. While some cyber-events may fall within the § 748.1(b) definition of catastrophic act, the Board believes they are sufficiently distinguishable and distinct to warrant separate consideration. The Board further believes that the longstanding requirement that FICUs be given five business days to report catastrophic acts, as defined in § 748.1(b), is still appropriate. However, the agency will continue to monitor the issue after this rule goes into effect, in the event clarification is needed.

With regard to Appendix B guidance, one commenter stated that Appendix B should be amended to state that it does not supersede this rule. Another commenter stated that the NCUA should remove the Appendix B language that refers to reporting to a FICU's regional director because most reportable incidents covered by Appendix B will be covered by this rule.

The Board does not intend to amend Appendix B at this time. However, Appendix B provides guidance on FICUs' obligations under § 748.0 and applicable statutes and, thus, does not supersede this rule.[21] If a FICU experiences a *reportable cyber incident*, that incident shall be reported under the requirements of this rule.

Finally, another commenter stated that while there is some overlap with existing Part 748 reporting requirements, the overlap is minimal, and the proposed rule sufficiently clarifies the requirements of each.

With regard to the definition of vital member services, one commenter stated that the definition needs to be updated to reflect changes in how vital services are delivered to members. Another commenter stated that the NCUA should not require reporting for non-malicious system outages; for example, incidents that involve a substantial loss of availability of a network that disrupts vital member services when a FICU undertakes a technology transition or system upgrade. In these situations, the commenter stated that reporting to the FICU's board of directors should be sufficient.

The NCUA recognizes that FICUs will have planned updates and planned outages that will not require notification. However, a failed system upgrade that causes widespread unplanned outages for members would be reportable under this final rule.

Coordination with the states and other agencies

Five commenters stated that it is important to coordinate with other regulatory agencies to minimize redundancy and inconsistency. One of these commenters specifically noted the importance of coordinating with state regulators. One commenter encouraged the NCUA to engage with the Financial Services Information Sharing and Analysis Center. Another commenter noted the importance of coordinating with CISA and the U.S. Treasury to ensure harmonization with the Cyber Incident Reporting Act.

---

[21] The Board's final rule on the role of supervisory guidance provides further discussion on the role and use of guidance in the supervisory process. 86 FR 7949 (Feb. 3, 2021)

The final rule does not prevent existing supervisory information sharing frameworks. The Board agrees that voluntary information sharing is important and encourages FICUs to continue sharing information through established channels. The agency intends to coordinate with CISA, state and federal regulators, and the U.S. Treasury as much as possible.

Policy expectations

Two commenters noted that it is important for the NCUA to define what its policy expectations are, to issue supervisory guidance for institutions to review in developing their policies and procedures, and to show how examiners will assess reported incidents during the annual exam. One commenter stated that it is unclear what follow up action the NCUA is expecting and, thus, this represents an unaccounted impact on FICUs. This commenter also suggested the NCUA create a safe harbor for FICUs that make good faith efforts to perform a reasonable assessment of a cyber incident.

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.

Ransomware

Five commenters mentioned ransomware. Two commenters stated that ransomware reporting should be the same as for other cyber incidents. One commenter supported a shorter window for ransomware reporting. One commenter stated that the NCUA should follow CISA, and one commenter said more specifically that the agency should wait until we know how CISA will handle ransomware reporting.

Notification to the agency of ransomware incidents should be the same as the reporting required under this rule for other cyber incidents. While the Cyber Incident Reporting Act does require entities to report ransomware *payments* within 24-hours, CISA has not yet promulgated regulations to that effect and this rule does not create a separate reporting framework for

ransomware payments. However, the Board encourages FICUs to contact law enforcement and CISA, as appropriate, in the event of a cyber incident that may be criminal in nature.

Application to federally chartered corporate credit unions and federally insured, state-chartered corporate credit unions

The proposed rule applied to federally chartered and federally insured, state-chartered corporate credit unions. Only one commenter mentioned this point and stated that they support such application. The final rule does not amend this aspect of the proposed rule. Thus, the final rule applies to all FICUs including all federally insured corporate credit unions.

V. Regulatory Procedures

A. Regulatory Flexibility Act

The Regulatory Flexibility Act requires the NCUA to prepare an analysis to describe any significant economic impact a regulation may have on a substantial number of small entities.[22] For purposes of this analysis, the NCUA considers small credit unions to be those having under $100 million in assets.[23] The final rule requires a FICU to notify the NCUA upon experiencing a substantial cyber incident. This notification requirement is not expected to increase cost burdens on FICUs as it requires only that FICUs provide an early notification to the agency without requiring any detailed assessments or evaluations. Also, while the final rule could lead to cost savings for FICUs if the NCUA or other government agencies can help to mitigate the impact of a cyber incident, the Board does not expect the final rule to accord a significant economic benefit to a substantial number of FICUs. Accordingly, the NCUA certifies that the final rule will not have a significant economic impact on a substantial number of small credit unions.

B. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 et seq.) requires that the Office of Management and Budget (OMB) approve all collections of information by a Federal

---

[22] 5 U.S.C. 603(a).
[23] 80 FR 57512 (Sept. 24, 2015).

agency from the public before they can be implemented. Respondents are not required to respond to any collection of information unless it displays a valid OMB control number. In accordance with the PRA, the information collection requirements included in this final rule have been submitted to OMB for approval under control number 3133-0033, Security Program, 12 CFR 748.

C. Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on state and local interests. In adherence to fundamental federalism principles, the NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5), voluntarily complies with the Executive order. This rulemaking will not have a substantial direct effect on the states, on the connection between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. Although the final rule applies to federally insured, state-chartered credit unions (FISCUs), it imposes only a minimal reporting requirement and does not affect the ability of state regulatory agencies to regulate, supervise, or examine FISCUs on this subject. Therefore, the NCUA has determined that this final rule does not constitute a policy that has federalism implications for purposes of the Executive order.

D. Assessment of Federal Regulations and Policies on Families

The NCUA has determined that this final rule will not affect family well-being within the meaning of Section 654 of the Treasury and General Government Appropriations Act, 1999.[24]

E. Small Business Regulatory Enforcement Fairness Act

The Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA) generally provides for congressional review of agency rules.[25] A reporting requirement is triggered in instances where the NCUA issues a final rule as defined by section 551 of the Administrative

[24] Pub. L. 105–277, 112 Stat. 2681 (1998).
[25] 5 U.S.C. 551.

Procedure Act. An agency rule, in addition to being subject to congressional oversight, may also be subject to a delayed effective date if the rule is a "major rule." The NCUA does not believe this rule is a "major rule" within the meaning of the relevant sections of SBREFA. As required by SBREFA, the NCUA will submit this final rule to OMB for it to determine whether the final rule is a "major rule" for purposes of SBREFA. The NCUA also will file appropriate reports with Congress and the Government Accountability Office so this rule may be reviewed.

For purposes of the Congressional Review Act, the OMB makes a determination as to whether a final rule constitutes a "major rule." If a rule is deemed a "major rule" by the OMB, the Congressional Review Act generally provides that the rule may not take effect until at least 60 days following its publication. The Congressional Review Act defines a "major rule" as any rule that the Administrator of the Office of Information and Regulatory Affairs of the OMB finds has resulted in or is likely to result in (1) an annual effect on the economy of $100 million or more; (2) a major increase in costs or prices for consumers, individual industries, Federal, State, or local government agencies or geographic regions, or (3) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of U.S.-based enterprises to compete with foreign-based enterprises in domestic and export markets.[26]

List of Subjects in 12 CFR Part 748

Computer technology, Confidential business information, Credit unions, Internet, Personally identifiable information, Privacy, Reporting and recordkeeping requirements, Security measures

By the NCUA Board on February 16, 2023.

Melane Conyers-Ausbrooks,

[26] 5 U.S.C. 804(2).

Secretary of the Board.

For the reasons stated in the preamble, the NCUA Board amends 12 CFR part 748, as follows:

PART 748 – SECURITY PROGRAM, SUSPICIOUS TRANSACTIONS, CATASTROPHIC ACTS, CYBER INCIDENTS, AND BANK SECRECY ACT COMPLIANCE.

1. The authority citation for part 748 is revised to read as follows:

Authority: 12 U.S.C. 1766(a), 1786(b)(1), 1786(q), 1789(a)(11); 15 U.S.C. 6801-6809; 31 U.S.C. 5311 and 5318.

2. Revise the heading for part 748 to read as set forth above.

3. Amend § 748.1 as follows:

a. Redesignate paragraph (c) as paragraph (d); and

b. Add a new paragraph (c).

The addition reads as follows:

§ 748.1 Filing of reports.

* * * * *

(c) *Cyber incident report.* Each federally insured credit union must notify the appropriate NCUA-designated point of contact of the occurrence of a *reportable cyber incident* via email, telephone, or other similar methods that the NCUA may prescribe. The NCUA must receive this notification as soon as possible but no later than 72 hours after a federally insured credit union reasonably believes that it has experienced a reportable cyber incident or, if reporting pursuant to paragraph (c)(1)(i)(C) of this section, within 72 hours of being notified by a third-party, whichever is sooner.

(1) *Reportable cyber incident.* (i) A reportable cyber incident is any substantial cyber incident that leads to one or more of the following:

(A) A substantial loss of confidentiality, integrity, or availability of a network or member information system as defined in appendix A, section I.B.2. e., of this part that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services as defined in § 749.1 of this chapter, or has a serious impact on the safety and resiliency of operational systems and processes.

(B) A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.

(C) 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.

(ii) 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.

(2) *Definitions*. For purposes of this part:

Compromise means the unauthorized disclosure, modification, substitution, or use of sensitive data or the unauthorized modification of a security-related system, device, or process in order to gain unauthorized access.

Confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

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.

Cyberattack means an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Disruption means an unplanned event that causes an information system to be inoperable for a length of time.

Integrity means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Sensitive data means 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.

* * * * *

4. Amend appendix B to part 748 as follows:

a. Redesignate footnotes 29 through 42 as footnotes 1 through 14;

b. In the introductory text of section I:

i. Revise the first sentence; and

ii. Remove "Part 748" and add "this part" in its place; and

c. Revise newly redesignated footnotes 1 and 11.

The revisions read as follows:

Appendix B to Part 748 - Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

I. * * *

This appendix provides guidance on NCUA's Security Program, Suspicious Transactions, Catastrophic Acts, Cyber Incidents, and Bank Secrecy Act Compliance regulation,[1]

interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLBA"), and describes response programs, including member notification procedures, that a federally insured credit union should develop and implement to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member. * * *

* * * * *

[1]This part.

* * * * *

[11]A credit union's obligation to file a SAR is set forth in § 748.1(d).

* * * *

[FR Doc. 2023-03682 Filed: 2/28/2023 8:45 am; Publication Date: 3/1/2023]