**7535-01-U**

**NATIONAL CREDIT UNION ADMINISTRATION**

**12 CFR Part 748**

**NCUA-2022-0099**

**RIN: 3133-AF47**

**Cyber Incident Notification Requirements for Federally Insured Credit Unions**

**AGENCY:** National Credit Union Administration (NCUA)

**ACTION:** Proposed rule

**SUMMARY:** Due to the increased frequency and severity of cyberattacks on the financial services sector, the NCUA Board is proposing to require 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 federally insured credit union reasonably believes that it has experienced a reportable cyber incident. This notification requirement provides an early alert to the NCUA and does not require credit unions to provide a detailed incident assessment to the NCUA within the 72-hour time frame.

**DATES:** Comments must be received on or before [INSERT DATE 60 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit written comments, identified by RIN 3133-AF47, by any of the following methods (**Please send comments by one method only**):

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments for NCUA-2022-0099.
- Fax: (703) 518-6319. Include "[Your Name]—Comments on Proposed Rule: Cyber Incident Notification Requirements for Federally Insured Credit Unions" in the transmittal.
- Mail: Address to Melane Conyers-Ausbrooks, Secretary of the Board, National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314-3428.

**PUBLIC INSPECTION:** You may view all public comments on the Federal eRulemaking Portal at http://www.regulations.gov as submitted, except for those we cannot post for technical reasons. The NCUA will not edit or remove any identifying or contact information from the public comments submitted. Due to COVID-19 safety measures in effect, the usual opportunity to inspect paper copies of comments in the NCUA's law library is not currently available. After these safety measures are relaxed, visitors may make an appointment to review paper copies by calling (703) 518-6540 or e-mailing OGCMail@ncua.gov.

**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. Background**

**II. Proposed Rule**

**III. Review of Existing Regulations and Guidance**

**IV. Legal Authority**

**V. Request for Comments**

**VI. Regulatory Procedures**


## I. Background

Given the frequency and severity of cyber incidents within the financial services industry, the National Credit Union Administration Board (Board) believes it is important that the National Credit Union Administration (NCUA or agency) be notified of cyber incidents that disrupt a federally insured credit union's (FICU) operations, lead to unauthorized access to sensitive data, or disrupt members' access to accounts or services. In accordance with § 704.1(a) of the NCUA's rules and regulations, this proposed rule also applies to federally chartered corporate credit unions and federally insured, state-chartered corporate credit unions.

Cyberattacks reported to federal law enforcement have increased in frequency and severity in recent years.[1] The financial services sector is one of the top U.S. critical

[1] *See* Federal Bureau of Investigation, Internet Crime Complaint Center, 2021 Internet Crime Report, citing a seven-percent increase in complaints of suspected internet crime with the top three cyber-crimes reported by victims being phishing scams, non-payment/non-delivery scams, and personal data breach, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

infrastructure sectors targeted by ransomware.[2] Cyberattacks may use destructive malware or other malicious software to target weaknesses in the computers or networks of financial institutions, typically with malicious intent.

Some cyberattacks have the potential to alter, delete, or otherwise render a credit union's data and systems unusable. Examples include a large-scale distributed denial of service (DDoS) attack that disrupts member account access, a computer hacking incident that disables business operations, or a data breach that exposes sensitive data. Depending on the scope of a cyber incident, a credit union's data and system backups may also be affected which can severely affect the ability of the credit union to recover operations. Cyber incidents can result from destructive malware or malicious software (cyberattacks), as well as non-malicious failure of hardware or software, personnel errors, and other causes.

A FICU experiencing a cyber incident is encouraged to contact relevant law enforcement or security agencies, as appropriate, after the incident occurs. Furthermore, providing information on cyber intrusions or other cyber incidents to the NCUA, the Federal Bureau of Investigation, and the Cybersecurity and Infrastructure Security Agency (CISA)[3] provides the U.S. government with information that can be used to identify new cyber-related adversarial tactics, techniques, and procedures, as well as information on industry sectors that are being targeted. This leads to greater visibility and an ability for the U.S. government to issue cybersecurity alerts, advise software and equipment manufacturers of critical vulnerabilities, and prosecute offenders.

---

[2] *Id.* at 15.
[3] CISA, Department of Homeland Security – Fact Sheet. *See* https://www.cisa.gov/sites/default/files/publications/CISA-Factsheet_16-Dec-2021-V4_508.pdf.

## II. Proposed Rule

The NCUA Board is issuing this notice of proposed rulemaking (proposal or proposed rule) to require a FICU to provide the NCUA with prompt notification of any *cyber incident* that rises to the level of a *reportable cyber incident*. 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.[4]

The proposed rule defines *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.[5]

The proposed rule defines a *reportable cyber incident* as:

Any substantial cyber incident that leads to one or more of the following:

---

[4] The Cyber Incident Reporting for Critical Infrastructure Act of 2022, part of the Consolidated Appropriations Act of 2022, will require a covered entity to report a covered cyber incident to CISA not later than 72 hours after the entity reasonably believes that the covered cyber incident has occurred. Consolidated Appropriations Act of 2022, Division Y, Pub. L. 117–103 (Mar. 15, 2022), *available at* https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[5] 6 U.S.C. 659(a)(5).

- A substantial loss of confidentiality,[6] integrity,[7] or availability of a network or member information system[8] that results from the unauthorized access to or exposure of sensitive data,[9] disrupts[10] vital member services,[11] 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[12] or exploitation of vulnerabilities.

- A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise[13] of a credit

---

[6] *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 proposing to use 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.

[7] *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.

[8] *Member information system* means any method used to access, collect, store, use, transmit, protect, or dispose of member information. 12 CFR 748, App. A(I)(B)(2)(e).

[9] The NCUA proposes to define *sensitive data* 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.

[10] 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.

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

[12] *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.

[13] 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.

union service organization, cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise.

Excludes—

- any event where the cyber incident is performed in good faith by an entity in response to a specific request by the owner or operator of the information system.

The proposed definition of *reportable cyber incident* is intended to capture the reporting of substantial cyber incidents. What a FICU would consider to be *substantial* will likely depend on a variety of factors, including the size of the FICU, the type and impact of the loss, and its duration, for example. The agency expects a FICU to exercise reasonable judgment in determining whether it has experienced a substantial cyber incident that would be reportable to the agency. Under this proposal, if a FICU is unsure as to whether a cyber incident is reportable, the Board encourages the FICU to contact the agency.

The first prong of the *reportable cyber incident* definition would require a FICU 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 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. Only a cyber incident that leads to a substantial loss of confidentiality, integrity, or availability would be reportable to the agency.

The second prong of the *reportable cyber incident* definition would 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 DDoS attack that disrupts member account access would be reportable under this prong. Blocked phishing attempts, failed attempts to gain access to systems, or unsuccessful malware attacks would not be reportable.

The third prong of the *reportable cyber incident* definition would require a FICU to notify the agency either when a third-party service provider has informed a FICU that the FICU's sensitive data or business operations have been compromised as a result of a cyber incident experienced by the third-party service provider or upon the FICU forming a reasonable belief this has occurred, whichever occurs sooner.

Credit unions are increasingly using third parties to provide technological services, including information security and mobile and online banking. These third-party systems and servers also store a vast amount of FICU member data. A compromise of a third party's systems

can be the result of an intentional cyberattack or an unintentional disclosure or loss of information. Considering the high degree of reliance by FICUs upon third parties, it is imperative that the NCUA be informed of any type of compromise to a third party's systems that places the credit union system at risk. Systemic risk from third-party vendors and credit union service organizations (CUSO) is a significant concern given that credit unions rely on many of the same third-party vendors.

As of March 30, 2022, the top five credit union core processing system third-party vendors provided service to credit unions holding approximately 87 percent of total credit union system assets. Likewise, at the end of 2021, the top five CUSOs provided service to credit unions that hold approximately 95 percent of total credit union system assets. Significant problems or a failure with a critical vendor or CUSO has the potential to result in disruption, including losses, to many credit unions and, in turn, pose risk to the National Credit Union Share Insurance Fund (NCUSIF) and national economic security given the amount and type of data held and processed, as well as the number of Americans who use credit unions for financial services. Thus, when a FICU is alerted to a cyber incident caused by a third party which impacts the FICU's sensitive data or business operations, the FICU must report the incident to the NCUA as soon as possible but no later than 72 hours after it was notified by the third party or within 72 hours of the FICU forming a reasonable belief that a reportable cyber incident has occurred, whichever is sooner.

Finally, a FICU would 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.[14]

In addition to the preceding examples, the following is a non-exhaustive list of incidents that would be considered *reportable cyber incidents* under the proposed rule:

1. A computer hacking incident that disables a FICU's operations.
2. A ransom malware attack that encrypts a core banking system or backup data.
3. Third-party notification to a FICU that they have experienced a breach of a FICU employee's personally identifiable information (PII).
4. A detected, unauthorized intrusion into a network information system.
5. Discovery or identification of zero-day malware[15] in a network or information system.
6. Internal breach or data theft by an insider.
7. A systems compromise resulting from card skimming.
8. Sensitive data exfiltrated outside of the FICU or a contracted third party in an unauthorized manner, such as through a flash drive or online storage account.

The Board expects that FICUs would consider whether other cyber incidents they experience, beyond those listed above, constitute reportable cyber incidents for purposes of

---

[14] 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.

[15] Zero-day malware attack is a cyber-attack that exploits a previously unknown hardware, firmware, or software vulnerability. *See* https://csrc.nist.gov/glossary/term/zero_day_attack. This meets the first prong of a reportable cyber incident because there is a substantial loss of integrity of a network or member information system from unauthorized access.

notifying the NCUA. Under this proposal, if a FICU is unsure as to whether a cyber incident is reportable, the Board encourages the FICU to contact the agency.

A cyber incident reporting requirement will help promote early awareness of emerging threats to FICUs and the broader financial system. This early awareness will help the NCUA react to these threats before they become systemic. This reporting 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 agency will require only certain basic information, to the extent it is known to the FICU at the time of reporting, such as:

- A basic description of the reportable cyber incident, including what functions were, or are reasonably believed to have been, affected.
- The estimated date range during which the reportable cyber incident took place.
- Where applicable, a description of the exploited vulnerabilities and the techniques used to perpetrate the reportable cyber incident.
- Any identifying or contact information of the actor(s) reasonably believed to be responsible.
- The impact to the FICU's operations.

The NCUA anticipates that further follow-up communications between the FICU and the agency will occur through the supervisory process, as necessary. As such, the proposed rule does not include any prescribed reporting forms or templates, which should minimize reporting burden.

The Board does not expect that a FICU would typically be able to come to a reasonable belief that a reportable cyber incident has occurred immediately upon becoming aware of a cyber

incident. Rather, the Board anticipates that a FICU would take some time to form a reasonable belief that it has experienced a reportable cyber incident. The Board recognizes that a FICU may not be able to form a reasonable belief that a reportable cyber incident has occurred outside of normal business hours. 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 recognizes that a FICU may be working expeditiously to resolve the reportable cyber incident at the time it would be expected to notify the agency. Thus, the Board believes 72 hours is a reasonable amount of time to notify the agency upon the occurrence of a reportable cyber incident, particularly because the notice would not need to include a lengthy assessment of the incident. The Board also recognizes that these situations can be fluid and that additional information or changes to previously reported information may become available after the initial report. The Board expects only that FICUs share general information about what is known at the time.

While the Board is proposing a 72-hour time frame, depending on the feedback received during the comment period and the agency's analysis of the need for more prompt reporting, the final rule may provide a shorter time frame, such as 36 hours as the federal banking agencies require.[16] Moreover, the notice could be provided to a designated point of contact at the agency via email or telephone or other similar method that the agency may prescribe through guidance. This notification, and any information provided by a FICU related to the incident, would be subject to the NCUA's confidentiality rules.[17]

[16] 86 FR 66424 (Apr. 1, 2022).
[17] 12 CFR part 792.

Knowing about and responding to cyber incidents affecting FICUs is important to the NCUA's mission for a variety of reasons, including the following:

- The receipt of cyber incident information may give the NCUA earlier awareness of emerging threats to individual FICUs and, potentially, to the broader financial system.
- An incident may so severely impact a FICU that it can no longer support its members, and the incident could impact the safety and soundness of the FICU, leading to its failure. In these cases, the sooner the NCUA knows of the event, the better it can assess the extent of the threat and take appropriate action.
- An incident may substantially harm or inconvenience a FICU's members and undermine a FICU's consumer protection obligations. In these cases, the sooner the NCUA knows of the event, the sooner it can take appropriate action, including helping the FICU protect its members.
- Based on the NCUA's broad supervisory experience, it may be able to provide information and guidance to FICUs that may not have previously faced a particular type of cyber incident.
- The NCUA would be better able to conduct analyses across the credit union system to improve guidance, adjust supervisory programs, and provide information to the industry to help FICUs protect themselves.

- Receiving notice would enable the NCUA to facilitate requests from FICUs for assistance through the U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection.[18]

In March of this year, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Cyber Incident Reporting Act or Act). That Act requires CISA to publish a final rule by September 2025 that will require covered entities, as will be defined in that rule, to report certain cyber incidents to CISA not later than 72 hours after their occurrence.[19] 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.

The Board is proposing to make two technical conforming amendments to Appendix B to Part 748 to reflect the changes proposed in this rule. The first amends the Appendix's reference to the heading to Part 748. The second amends a footnote reference to the filing requirements for Suspicious Activity Reports (SARs).

The Board believes this proposed rule is necessary because, as discussed below, current reporting requirements, while related to cyber incidents in some instances, are neither designed nor intended to provide timely information to the NCUA about such incidents.

---

[18] The U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection coordinates with U.S. Government agencies to provide agreed-upon assistance to banking and other financial services sector organizations on cyber response and recovery efforts. These activities may include providing remote or in-person technical support to an organization experiencing a significant cyber-event to protect assets, mitigate vulnerabilities, recover and restore services, identify other entities at risk, and assess potential risk to the broader community. The Federal Financial Institutions Examination Council's Cybersecurity Resource Guide for Financial Institutions (Oct. 2018) identifies additional information available to banking organizations. *Available at* https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf.

[19] Consolidated Appropriations Act of 2022, *supra* note 4.

## III. Review of Existing Regulations and Guidance

The Board considered whether the information that would be provided under the proposed rule could be obtained through existing reporting standards. Currently, FICUs may be required to report certain instances of disruptive cyber-events and cyber-crimes by filing SARs.[20] In addition, FICUs should notify the appropriate NCUA Regional Director "as soon as possible" when they become aware "of an incident involving unauthorized access to or use of sensitive member information."[21] FICUs are also required to notify the NCUA within five business days of any catastrophic act that occurs at their office(s).[22]

These reporting provisions can provide the NCUA with valuable insight into cyber-related events and information-security compromises; however, they do not provide the agency with sufficiently timely information about every substantial cyber incident that would be captured by the proposed rule.

Under the reporting requirements of the Bank Secrecy Act (BSA) and its implementing regulations, FICUs are required to file SARs when they detect a known or suspected criminal violation of federal law or a suspicious transaction related to a money-laundering activity.[23] SARs, however, serve a different purpose from this proposed cyber notification requirement and do not require reporting of every incident captured by the proposed definition of a reportable cyber incident. Moreover, the 30-calendar-day reporting requirement under the BSA framework

[20] 12 CFR 748.1(c).
[21] 12 CFR 748, App. B(II)(A)(1)(b).
[22] 12 CFR 748.1(b).
[23] *See, e.g.,* 31 U.S.C. 5311 *et seq.;* 31 CFR subtitle B, chapter X; 12 CFR 748.1(c).

(with an additional 30 calendar days provided in certain circumstances) does not provide the agency with sufficiently timely notice of reported incidents.

Under the reporting guidelines set forth in Appendix B of Part 748, the NCUA's Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice (Unauthorized Access Guidance), a FICU's procedures should include notifying the appropriate NCUA Regional Director or, in the case of state-chartered credit unions the appropriate state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information.[24] While this may provide the agency with notice of some cyber incidents, this standard is too narrow in scope to address all relevant cyber incidents of which the NCUA needs to be notified. In particular, the Gramm-Leach-Bliley Act (GLBA) notification standard, on which the Unauthorized Access Guidance is based, does not include the reporting of incidents that disrupt operations or compromise sensitive credit union data but do not compromise sensitive member information.

At the same time, this proposed rule's definition of 'sensitive data' contains some overlap with the definition of 'member information' used in the Unauthorized Access Guidance. Thus, there may be instances where unauthorized access to or use of sensitive member information could trigger FICU reporting to the NCUA pursuant to the Unauthorized Access Guidance as well as reporting to the NCUA under this proposed rule. In such instances, the agency expects FICUs to use the reporting framework outlined in this proposed rule. Despite this potential for

[24] 12 CFR 748, App. B(II)(A)(1)(b), interpreting the Gramm-Leach-Bliley Act, 15 U.S.C. 6801(b).

overlap in some instances, the agency continues to find the Unauthorized Access Guidance to be applicable and appropriate for complying with GLBA and Part 748.

Finally, the NCUA regulations require a FICU to notify the appropriate NCUA Regional Director within five business days of any catastrophic act that occurs at its office(s). The NCUA regulations define a catastrophic act as "any disaster, natural or otherwise, resulting in physical destruction or damage to the credit union or causing an interruption in vital member services, as defined in § 749.1 of this chapter, projected to last more than two consecutive business days."[25] In 2007, the NCUA amended the definition of *catastrophic act* "to address concerns that relatively minor events could be construed to trigger the need to file a report and, also, clarifying the causal link between a disaster and an interruption in vital member services."[26] The Board believed these changes to be "consistent with the usual and customary meaning of the word catastrophe."[27] Furthermore, "[t]hese changes also reinforce the Board's view that the reporting requirement applies only to a disaster as opposed to a circumstance where physical damage or a business closing occurs but is not disaster-related."[28]

---

[25] 12 CFR 748.1(b). *See also* 12 CFR 749, App. B, Catastrophic Act Preparedness Guidelines. The NCUA has long required catastrophic act reporting. In 1970, Congress amended the Federal Credit Union Act (FCUA) to require that the NCUA promulgate rules establishing minimum standards for the installation, maintenance, and operation of security devices and procedures to discourage robberies, burglaries, and larcenies. The 1970 amendment to the FCUA also required the agency to adopt time limits for compliance and mandated the submission of periodic reports. *See* 12 U.S.C. 1785(e) (P.L. 91-468) (84 Stat. 1002). Thus, since 1971, the NCUA has promulgated regulations requiring the submission of reports within five working days of an occurrence, or attempted occurrence, of a crime or catastrophic act. *See* 36 FR 10940 (June 1, 1971). *See also* 47 FR 17981 (Apr. 27, 1982); 50 FR 53295 (Dec. 31, 1985). In 1996, the NCUA and the federal banking agencies, working with the U.S. Treasury's Financial Crimes Enforcement Network, replaced the crime reporting requirement, or "Criminal Referral Form" as it was known, with a new, more simplified "Suspicious Activity Report" for reporting known or suspected federal criminal law violations and suspicious currency transactions. *See* 61 FR 11527 (Mar. 21, 1996).
[26] 72 FR 42271 (Aug. 2, 2007).
[27] *Id.*
[28] *Id.*

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.

## IV. Legal Authority

The Board issues this proposed 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.[29] 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.[30] Accordingly, the FCUA grants the Board broad rulemaking authority to ensure that the credit union industry and the NCUSIF remain safe and sound.

## V. Request for Comments

[29] 12 U.S.C. 1789(a)(11).
[30] 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).

The Board may amend the final rule based on comments received in response to this proposed rule. The Board seeks comment on all parts of the proposed rule, including the following:

1. The concepts used in the definition of *reportable cyber incident* are as defined currently in the NCUA regulations or as defined by the National Institute of Standards and Technology. Are these appropriate concepts and definitions to use? If not, please explain your reasoning and how the proposed definition of *reportable cyber incident* should be modified.
2. The proposed definition of *reportable cyber incident* would require a FICU to notify the NCUA in the event of a substantial cyber incident or cyberattack. What, if any, challenges would a FICU experience in concluding that it has experienced a cyberattack after determining it has experienced a reportable cyber incident? Would including a definition of *substantial* help a FICU in determining if it experienced a reportable cyber incident? If so, how would you define substantial?
3. The proposed definition of *reportable cyber incident* would require FICUs to notify the NCUA in the event of a third-party compromise that impacts the FICU's data or operations. In your experience, how do third parties with which FICUs contract currently provide notice when such incidents occur?
4. The federal banking agencies recently promulgated a rule that requires banking organizations to report certain computer-security incidents to their regulators within 36 hours.[31] After the federal banking agencies' rule was finalized, Congress enacted

[31] 86 FR 66424 (Apr. 1, 2022).

the Cyber Incident Reporting Act, which contains a 72-hour reporting window. Should the NCUA adopt a 72-hour reporting window, as proposed, or 36 hours as the federal banking agencies adopted, or is a different time frame warranted? If a different time frame, please explain what that would be and why?

5. How should FICUs notify the NCUA when faced with a reportable cyber incident? Are email and telephone the best methods as suggested in the proposal? Should the NCUA adopt a single method of cyber incident reporting? Should the NCUA adopt a single point of contact in its Central Office or should FICUs report to their respective NCUA regional offices?
6. The Cyber Incident Reporting Act requires CISA to establish separate reporting requirements for ransomware attacks. The Act defines a ransomware attack as an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism, such as a denial-of-service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system, to extort a demand for a ransom payment. The reporting window for these types of incidents is 24 hours. Should the NCUA incorporate a similar reporting requirement of 24 hours specifically for ransomware attacks?
7. In addition to those referenced in the proposed rule, are there any other existing regulatory provisions that should be amended or clarified as a result of the proposed cyber-incident reporting requirement? For example, should § 748.1(b) on catastrophic act reporting be amended to include a requirement to report unplanned

systemic outages of technological assets and critical networks, computer assets, systems, data, devices, or applications used to deliver vital electronic services to credit union members, not related to cyber incidents, that last more than two consecutive business days? For example, should the definition of vital member services be updated to reflect changes in how vital services are delivered to members to include reliance on the use of electronic banking systems and/or mobile banking applications to access and conduct transactions on their share, deposit, or loan accounts?

8. Is further clarification needed about any potential overlap between this proposed rule's reporting requirement in the event of unauthorized access to or exposure of sensitive data and the reporting of unauthorized access to member information conducted under the Unauthorized Access Guidance? If so, please provide specific concerns or issues that need to be addressed.
9. The NCUA invites comments on specific examples of incidents that should or should not constitute *reportable cyber incidents*. In addition to the examples listed in the proposal are there others the agency should consider?

## VI. Regulatory Procedures

### *A. Regulatory Flexibility Act*

The Regulatory Flexibility Act (RFA) generally requires that, in connection with a notice of proposed rulemaking, an agency prepare and make available for public comment an initial regulatory flexibility analysis that describes the impact of a proposed rule on small entities. A regulatory flexibility analysis is not required, however, if the agency certifies that the rule will

not have a significant economic impact on a substantial number of small entities (defined for purposes of the RFA to include FICUs with assets less than $100 million)[32] and publishes its certification and a short explanatory statement in the Federal Register together with the rule. The proposed rule would require FICUs to 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. While this notice requirement is more than currently required under the agency's regulations, the proposed rule is not expected to create a significant cost burden for FICUs. The proposed rule requires a FICU only to provide the agency with notice in the event of a reportable cyber incident. The initial notice only includes limited details of what is known at the time and is not a full assessment or analysis of the incident. Accordingly, the NCUA certifies that the proposed 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) applies to rulemakings in which an agency creates a new or amends existing information collection requirements.[33] For the purpose of the PRA, an information collection requirement may take the form of a reporting, recordkeeping, or a third-party disclosure requirement. The proposed rule does contain information collection requirements that require approval by the Office of Management and Budget under the PRA.[34] The proposed rule would require FICUs to notify the appropriate NCUA-designated point of

[32] NCUA Interpretive Ruling and Policy Statement 15–1, 80 FR 57512 (Sept. 24, 2015).
[33] 44 U.S.C. 3507(d); 5 CFR part 1320.
[34] 44 U.S.C. Chap. 35.

contact of the occurrence of a reportable cyber incident via email, telephone, or other similar methods that the NCUA may prescribe.

The information collection requirements associated with 12 CFR part 748 are cleared under OMB control number 3133-0033 and provide for catastrophic act reporting and GLBA incident reporting guidance under Appendix B to part 748. The proposed rule adds a cyber incident reporting under § 748.1(c) where FICUs would be required to report these incidents, as defined. The burden associated with the reporting requirements identified under Appendix B will be removed because most reporting will now fall under the new cyber incident requirement. The NCUA estimates a one-hour annual reporting burden on each FICU, for a total of 4,903 hours.

Adjustment will also be made to the information collection requirements under part 748 to reflect a reduction in the current number of FICUs and to provide for a more accurate response rate per respondent.

OMB Number: 3133-0033.

Title: Security Program, 12 CFR Part 748.

Type of Review: Revision of a currently approved collection.

Abstract: In accordance with Title V of GLBA, as implemented by 12 CFR part 748, FICUs are required to implement an information security program designed to protect member information. This information collection requires that such programs be designed to respond to incidents of unauthorized access or use, in order to prevent substantial harm or serious inconvenience to members. Part 748 sets forth the minimum requirements of a security program.

It also addresses member notification, filing with the Financial Crimes Enforcement Network, and monitoring BSA compliance.

Affected Public: Private Sector: Not-for-profit institutions

Estimated No. of Respondents: 4,903

Estimated No. of Responses per Respondent: 19

Estimated Total Annual Responses: 93,307

Estimated Burden Hours per Response: 2.58

Estimated Total Annual Burden Hours: 240,397

The NCUA invites comments on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (b) the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (c) ways to enhance the quality, utility and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology; and (e) estimates of capital or start-up costs and cost of operation, maintenance, and purchase of services to provide information.

All comments are a matter of public record. Interested persons are invited to submit written comments to (1) www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting the Agency under "Currently under Review," and (2) Dawn Wolfgang,

National Credit Union Administration, 1775 Duke Street, Suite 6032, Alexandria, Virginia 22314; Fax No. 703-519-8579; or email at PRAComments@ncua.gov. Given the limited in-house staff because of the COVID-19 pandemic, email comments are preferred.

*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. The NCUA has determined that this proposal 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.[35]

**List of Subjects in 12 CFR Part 748**

Credit unions; reporting and recordkeeping requirements; computer technology; internet; security measures; privacy; personally identifiable information; confidential business information

Authority and Issuance

[35] Pub. L. 105–277, 112 Stat. 2681 (1998).

By the National Credit Union Administration Board on ____, 2022.

_____

Melane Conyers-Ausbrooks
Secretary of the Board

For the reasons stated in the preamble, the NCUA proposes to amend 12 CFR Part 748, as follows:

1. The part heading for Part 748 is revised to read as follows:

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

2. 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.

3. Paragraph 748.1(c) is redesignated as 748.1(d) and a new paragraph (c) is added 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 section (c)(1)(iii), within 72 hours of being notified by a third party, whichever is sooner.

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

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

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

(iii) 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.

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.

*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.

*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.

*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. The first sentence of Appendix B to Part 748 is revised to read as follows:

*  *  *

This Guidance in the form of appendix B to NCUA's Security Program, Suspicious Transactions, Catastrophic Acts, Cyber Incidents, and Bank Secrecy Act Compliance regulation,[29] 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.

*  *  *

---

[29] 12 CFR Part 748.

5. Footnote 39 of Appendix B to Part 748 is revised to read as follows:

*  *  *

A credit union's obligation to file a SAR is set forth in 12 CFR Part 748.1(d).

*  *  *