3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

September 26, 2022

Melane Conyers-Ausbrooks
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314-3428

Re: Cyber Incident Notification Requirements for Federally Insured Credit Unions; (RIN 3133-AF47)

Dear Ms. Conyers-Ausbrooks:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response to the proposed rule issued by the National Credit Union Administration (NCUA) establishing a 72-hour period for a federally insured credit union (FICU) to provide notice of a reportable cyber incident after a reasonable determination is made that such an incident has occurred. NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve 133 million consumers with personal and small business financial service products.

NAFCU supports efforts to improve the resilience and operational integrity of the credit union system by promoting effective cybersecurity practices and early warning capabilities. NAFCU also encourages the harmonization of cybersecurity standards and recognizes that future implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) could ultimately incentivize alignment around a 72-hour reporting period. However, given that the Cybersecurity and Infrastructure Security Agency (CISA) has not yet engaged in a formal rulemaking to implement this future cyber reporting standard, and the agency is currently soliciting input on parameters for a future proposal, the NCUA's separate development of a similar cyber incident reporting standard may be premature and could possibly result in conflict with eventual CISA standards.[1]

Executive Summary

In general, the proposed timeframe for notifying the NCUA of a reportable cyber incident will correspond with additional administrative burden for credit unions. The overall magnitude of this burden will depend on a variety of factors such as the IT resources of the credit union, the threshold for reporting incidents, and the frequency of supervisory communication that transpires after an initial notice is made. To ease future compliance and ensure that administrative functions do not displace the core task of performing effective cybersecurity, NAFCU offers the following recommendations:

[1] *See* Department of Homeland Security, Cyber Incident Reporting for Critical Infrastructure Act of 2022 Listening Sessions, 87 Fed. Reg. 55830 (September 12, 2022)

1. Recognize a compliance safe harbor for a credit union that makes good faith efforts to perform a reasonable assessment of a cyber incident.
2. Provide additional clarification of core terminology, such as by defining a reportable cyber incident in a way that recognizes concepts of materiality and substantial harm.
3. Avoid prescriptive reporting templates, lengthy assessments, or excessive follow-up requests in favor of streamlined communication with supervisory teams.
4. Clarify the relationship between overlapping NCUA reporting standards to achieve regulatory harmonization, promote organizational coherence, and avoid redundant reporting obligations.
5. Avoid duplicate or inconsistent reporting with respect to the CIRCIA and future CISA rules, such as by recognizing that implementation of a 72-hour reporting framework may reflect an appropriate statutory anchor but could also be subject to additional regulatory tailoring to minimize administrative burden.
6. For third party cyber incidents, recognize that a credit union will have final say with respect to the question of whether a reportable cyber incident has occurred.
7. Tailor reporting thresholds to avoid imposing notification requirements for incidents that transpire far outside the domain of a credit union.
8. Ensure that appropriate coordination exists with other relevant federal regulators and that credit unions will be examined for data security compliance based on the standards and expectations communicated in Part 748 of NCUA's regulations.
9. Clearly state that cyber incident notifications submitted to the NCUA are confidential information exempt from public disclosure.

To the extent that the NCUA believes that issuing its own rule before CISA (which has a 2025 deadline) is necessary, NAFCU asks that the NCUA also ensure that the information collected from credit unions is used effectively to improve the security and resilience of the industry through timely and confidential information sharing. This goal could be accomplished by hosting more regular cybersecurity and threat intelligence briefings for credit union cybersecurity professionals.

Even if the NCUA decides not to proceed with a final rule at this time, it might also consider organizational enhancements to the appendices of Part 748 to improve accessibility and clarity. These changes might include consolidation of common definitions and principles within a unified Appendix. In the event the NCUA does proceed with a final rule, obviating duplicative notifications under overlapping frameworks will be paramount. NAFCU believes that these enhancements would help eliminate confusion that may exist when bifurcating general data security responsibilities from incident response.

General Comments

Credit unions dedicate massive resources to protect member information and continuously implement robust technical safeguards to ensure that sensitive data remains secure. Surveys of NAFCU members have revealed that credit union cybersecurity budgets have more than doubled over the past five years, and nearly all NAFCU members expect those same budgets to grow in the

future.[2] NAFCU's members also anticipate that cybersecurity risk will remain a top risk management concern in the coming years.

NAFCU supports efforts to strengthen the NCUA's ability to provide early warning to the industry of significant cyber threats. Coordination with federal law enforcement agencies, Treasury, and the Federal Financial Institutions Examination Council (FFIEC) agencies is an essential part of this capability, and the threat intelligence the NCUA can gather and share proactively serves as an important defense resource for credit unions.

While the proposed cyber incident reporting standard will no doubt improve the NCUA's ability to coordinate incident response activities across the industry, the NCUA should be mindful of balancing the administrative burden of additional reporting with the actual practice of effective cybersecurity. In this regard, NAFCU is appreciative of the proposal's emphasis that FICUs providing notice of a reportable incident share only "general information about what is known at the time" and that the notice itself "would not need to include a lengthy assessment."[3] However, it is still unclear what, if any, follow-up action would be pursued by the NCUA, which could represent an unaccounted impact on FICUs.

The proposed 72-hour reporting period for initial notifications aligns with statutory requirements in the CIRCIA; however, CISA has yet to adopt a final rule clarifying how this reporting standard will apply to "covered entities," as described in 6 U.S.C. § 681(5). Enacted in March 2022, the CIRCIA assigns to CISA the responsibility for implementing by 2025 a cyber reporting framework for critical infrastructure owners (covered entities). The statutory parameters for this framework will require covered entities to report "substantial" cyberattacks to CISA within 72 hours after forming a "reasonable belief" that a covered incident has occurred, and supplemental reports as new information becomes available. In addition, covered entities must report any ransomware payments to CISA within 24 hours of payment.

It is too early to tell how CISA might choose to moderate a future incident reporting standard based on the factors listed in 12 U.S.C. § 681(c), which require the agency to consider, among other things, "the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety."[4] A credit union that experiences a temporary system outage caused by user error, for example, would seem an unlikely source of disruption to the nation's financial sector critical infrastructure. Furthermore, while the NCUA's proposed reporting framework borrows its core structure from the CIRCIA, it does not account for any tailoring of regulatory expectations that may take shape in a future CISA rulemaking. Failure to consider applicable limits on reporting that CISA may eventually regard as reasonable for certain covered entities, such as small businesses, could place an undue burden on credit unions.

Although the NCUA regards it as "imprudent in light of the increasing frequency and severity of cyber incidents to postpone a notification requirement until after CISA promulgates a final rule,"

[2] *See* NAFCU, Report on Credit Unions, 48 (2021).
[3] NCUA, "Cyber Incident Notification Requirements for Federally Insured Credit Unions," 87 Fed. Reg. 45029, 45023 (July 27, 2022).
[4] 6 U.S.C. § 681(c)(1),

credit unions are already subject to multiple incident notification requirements. Credit unions must report disruptions to vital member services that result from catastrophic acts (which can include cyber related events), report certain incidents involving unauthorized access to member information, and must submit to FinCEN suspicious activity reports (SARs) when those transactions involve a cyber related event, such as a ransomware attack.[5] FinCEN's standard is especially broad since it advises credit unions that "[c]yber-events targeting financial institutions that ***could affect*** a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities" (emphasis added).[6]

The NCUA's claim that catastrophic act reporting offers an inadequate framework for cyber incidents suggests that the threshold for notification under the proposal must necessarily encompass even disruptions to non-vital member services.[7] Yet this broad net for reporting may—once again—overlook eventual tailoring by CISA as it contemplates appropriate limits on the regulatory definition of a covered cyber incident. For example, CISA must consider "the type, volume, and sensitivity of the data at issue," in a future rulemaking—qualities the NCUA proposal does not entirely address by merely adopting the CIRCIA's default statutory language.[8] Consequently, the NCUA may inadvertently develop a rule that is more burdensome than CISA's own standard for critical infrastructure entities. The risk of this occurring will almost certainly be greater if the NCUA finalizes its proposal before CISA has had an opportunity to gather input from financial sector stakeholders and develop its own rule, which is likely to serve as the anchor for future regulatory harmonization efforts within the financial sector.

The adoption of an even shorter, 36-hour period (referenced in the proposal) exemplifies the risk of abandoning the goal of regulatory harmonization. Not only would this unrealistic timeframe impair efforts to perform a reasonable assessment of a cyber incident, but it could also result in underreporting if internal processes for classifying an incident as reportable are aggressively tuned to rule out false positives as a means of managing administrative burden. To preserve an effective early warning capability, and one that is at least consistent with the CIRCIA's standard, the NCUA should not target a timeframe any shorter than 72-hours.[9]

With respect to post-notification communication with the NCUA, NAFCU recommends that the agency adopt a flexible supervisory process that is responsive to the facts and circumstances of a particular incident. When credit union cybersecurity resources are allocated to incident response and ongoing mitigation activities, the NCUA should not overburden credit unions with numerous follow-up communications, or demand detailed forensic information too soon after the initial notice is provided. If an incident remains unresolved and additional communication is necessary,

[5] *See* FinCEN, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, FIN-2016-A005 (October 25, 2016).
[6] *Id*.
[7] 87 Fed. Reg. 45033.
[8] 6 U.S.C. § 681b(c)(2)(B)(i)—(iii).
[9] The NCUA should also consider that the computer security incident notification requirement adopted by the other federal banking regulators in 2021 was adopted before the enactment of the CIRCIA, a development that would have likely changed the agencies' analysis concerning the benefits of regulatory harmonization. *See* 86 Fed. Reg. 66424, 66432 (November 21, 2021).

periodic dialogue with supervisory teams rather than repeat reporting would better conserve the critical IT security resources of a credit union.

Finally, as an overarching principle governing future compliance with the proposed reporting standard, the NCUA should recognize a safe harbor for FICU's that make good faith efforts to perform a reasonable assessment of a cyber incident. This safe harbor should give credit when a credit union has engaged key internal stakeholders (e.g., executive leaders, IT security professionals) during the investigative period. A safe harbor for good faith efforts would also align with the CIRCIA's guidelines for CISA with respect to future rulemaking and enforcement activity. The CIRCIA recognizes that in the context of cyber incident reporting, CISA should consider "the complexity in determining if a covered cyber incident has occurred" and only start the 72-hour reporting clock when a covered entity "reasonably believes" that a reportable cyber incident has occurred.[10] The proposal should reflect a similar understanding and the NCUA should afford deference to the expert judgment of credit union IT management when evaluating compliance with the proposed reporting standard.

Avoid duplicate or inconsistent reporting with respect to future implementation of the CIRCIA

Under the CIRCIA, an exception to filing a cyber incident or ransomware report directly with CISA is available when CISA has an existing agreement in place with a covered entity's federal regulator and the covered entity is required by law, regulation, or contract to report substantially similar information to its federal regulator within a substantially similar timeframe.[11] CIRCIA also establishes a Cyber Incident Reporting Council charged with reviewing "existing regulatory requirements, including the information required in such reports, to report incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements."[12]

In terms of CISA's implementation of rules governing the submission of supplemental reports, CIRCIA provides that the agency, in a future rulemaking, shall "consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable."[13] Collectively, these provisions emphasize principles of cybersecurity harmonization that NAFCU has long promoted.

To ensure that credit unions can fully benefit from the CIRCIA's provisions aimed at easing regulatory burden and avoiding duplication, NAFCU encourages the NCUA to coordinate with both CISA and Treasury to ensure that credit unions will only need to meet a single reporting standard administered by the NCUA. Although CISA has not yet issued a proposed rule to implement the CIRCIA, NAFCU acknowledges that general alignment around the 72-hour reporting period may be necessary to establish such a unified framework that supports one-time,

[10] 6 U.S.C. § 681b(a)(1); 6 U.S.C § 681d(e)(1).
[11] *See* 6 U.S.C. § 681b(a)(5)(B).
[12] 6 U.S.C § 681g(b)(1)
[13] *See* 6 U.S.C. § 681b(c)(7)(B).

pass-through reporting to the NCUA within a "substantially similar timeframe." However, alignment around this timeframe would be accomplished with greater certainty and with less risk of inconsistency if the NCUA were to wait until CISA has issued its own proposal based on stakeholder feedback.

With respect to a 24-hour ransomware payment reporting period, NAFCU recognizes that this standard was also established by the CIRCIA and that similar alignment of NCUA rules may eventually be necessary depending on the outcome of a future CISA rulemaking. However, NAFCU believes that it would be premature to establish ransomware reporting rules before CISA has developed its own standard which considers the availability of existing channels for obtaining substantially similar information.

CISA is likely to recognize in a future rulemaking credit unions' existing compliance with Part 748 of the NCUA's regulations and the Gramm-Leach-Bliley Act (GLBA). Consequently, CISA's regulatory implementation of a ransomware reporting standard may be adjusted to account for the industry's culture of compliance, close supervision, and overall cyber maturity. o. An NCUA rule addressing ransomware-specific reporting could deviate significantly from a future CISA standard. If the NCUA chooses to adopt ransomware provisions that must eventually change in response to a future CISA rulemaking, credit unions could be put in the position of having to operationalize a short-lived rule before transitioning to another.

To avoid unnecessary waste of credit union resources, NAFCU recommends the NCUA refrain from addressing ransomware-specific reporting until it has engaged with CISA to ensure that relevant requirements are aligned with CISA's expectations and fully considered the use of potential exemptions to unify and streamline ransomware reporting requirements. Deferral of a ransomware-specific component in the NCUA's proposal would not degrade the agency's ability to learn of ransomware events under the proposal's broad definition of a reportable cyber incident.

Recognizing that the proposal already ensures FICUs will provide timely notice of such events, NAFCU recommends the NCUA not incorporate a 24-hour reporting window that applies after ransomware payments are made.

Definition of reportable cyber incident and concept of "substantial"

The proposal defines a reportable cyber incident as any substantial cyber incident that involves the conditions listed in proposed § 748.1(c)(1)(i)(A)-(C). The term substantial is used not only in a general sense, but also incorporated within one of the components of the definition itself (i.e., "a substantial loss of confidentiality, integrity, or availability of a network"). As an initial matter, the NCUA should clarify how the term substantial applies to other component parts of the reportable cyber incident definition. For example, does a "disruption of business operations" described in § 748.1(c)(1)(i)(B) need to be substantial to be reportable? Likewise, does the term substantial modify the definition of "compromise" used in § 748.1(c)(1)(i)(C)? However the NCUA chooses to develop the definition of a reportable cyber incident, NAFCU asks that the agency grant appropriate deference to the reasonable judgment of credit unions.

Relatedly, the NCUA should clarify what characteristics of a cyber incident would make it a substantial incident. Ideally, such clarification would focus on principles-based factors rather than enumerate different types of data, systems or other static elements of an IT environment, which could quickly change in relative significance as cybersecurity best practices and mitigation strategies evolve. Recognizing that there is no one-size-fits-all approach to effective cybersecurity, NAFCU recommends clarifying the meaning of the term substantial in a way that aligns with concepts of materiality and substantial harm. This framing would better conform with the language used by other federal banking agencies in their final computer incident notification rule and the NCUA's own standard for reporting incidents of unauthorized access to sensitive information.[14]

An emphasis on the "materiality" of an incident and the FICU's certainty of substantial harm, incorporated within the definition of a reportable cyber incident, would be preferrable to a separate definition for the term substantial. By referencing an incident's material impact, the NCUA would better account for the scale and sophistication of individual credit unions. For example, a cyber incident (such as a service outage) when measured in terms of materiality might look different for a small credit union that serves several thousand members versus a credit union that serves several million. Likewise, by referencing a credit union's reasonable belief in the certainty of material harm occurring, the trigger for a reportable cyber incident will be clearer and less subjective as this better aligns with prevailing industry standards in the realm of enterprise risk management.

The NCUA should also clarify component terminology used to describe events that would trigger reporting obligations under the proposal. The definition of a reportable cyber incident incorporates the terms "disruption," "cyber incident," and "cyberattack," which are each defined separately. These terms include overlapping concepts which could create confusion when attempting to discern how each delimits reporting under specific factual circumstances. A cyber incident and cyberattack my cause disruption, but other causes of disruption—which may be natural, non-malicious, or not directly targeting a credit union or its vendors—may not be clearly understood as a reportable event.

For example, it may not be clear whether the NCUA should be notified if a power outage causes a disruption in member service if the cause of the disruption is determined to be a cyberattack at a utility company. While the proposal refers to supply chain *compromise* that could impact a CUSO, cloud service provider, or other third-party data hosting provider, the root cause of disruption may be attenuated beyond those listed entities.

Whether more attenuated forms of disruption are reportable may present an especially difficult question given that the proposed rule supplies no definition for "supply chain compromise." Under the CIRCIA the term is defined as "an incident within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or

[14] *See* Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," 86 Fed. Reg. 66424 at 66425 (November 11, 2021) (a notification incident is a computer-security incident that materially disrupts or degrades, or is reasonably likely to materially disrupt or degrade, covered services provided by a bank service provider); *see also* 12 CFR § 748 Appendix B ("Under Part 748.0, a credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member.")

availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle."[15] NAFCU recommends the NCUA align any definition of "supply chain compromise" with its statutory counterpart in the CIRCIA, but also recognize reasonable limits on the breadth of a credit union's information system supply chain.

Disruption caused by supply chain compromise could also be the result of an ongoing, but relatively low severity *cyberattack* affecting other sectors of the economy. Yet the resolution of such a cyberattack would be beyond the credit union's control and its length indeterminant, which could complicate initial assessments when reporting is required. Furthermore, the term cyberattack is defined in a way that does not consider the actual success or failure of the attack but focuses instead on the attack's occurrence and purpose (unlike the term cyber incident which considers the actual and imminent harm of an occurrence). Collectively, these ambiguities may result in a reporting framework where credit unions are not sure when to report certain incidents and how they should be described.

Another potential source of confusion is the FFIEC IT Handbook for Information Security, which provides a different definition of a "cyber attack."[16] Whereas the proposed definition offered by the NCUA focuses on an attack "targeting an enterprise's use of cyberspace," the FFIEC definition describes an attack "targeting an institution."[17] NAFCU recommends the NCUA align its definition of cyberattack more closely with the FFIEC definition, which more appropriately emphasizes the deliberate targeting of on an institution rather than other, unaffiliated entities that are not direct service providers. This would reduce reporting uncertainty in situations where cyber attacks do not intentionally target the credit union and have only an indirect impact on operations. In these situations, the current framework for reporting catastrophic acts already offers an appropriate framework for notifying the NCUA.

Lastly, the NCUA should consider limiting formal reporting for non-malicious system outages—events that are neither cyberattacks nor compromises but could potentially be reportable if they involve a substantial loss of availability of a network that disrupts vital member services. In these circumstances, more limited reporting to the affected credit union's board of directors would help alleviate administrative burden when a credit union undergoes a technology transition or system upgrade that may correspond with increased likelihood of prolonged service outage. In these cases, NAFCU believes that reporting to the NCUA is unnecessary given that the preamble of the proposal suggests that the agency's primary concern lies with cyberattacks and other malicious incidents.[18]

---

[15] 6 U.S.C. § 681(17).
[16] "An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network. An attack, via cyberspace, targeting an institution for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; destroying the integrity of the data; or stealing controlled information." FFIEC, Information Technology Examination Handbook: Information Security, 77 (September 2016).
[17] *See id.*
[18] NCUA, "Cyber Incident Notification Requirements for Federally Insured Credit Unions," 87 Fed. Reg. 45029 ("[P]roviding information on cyber intrusions or other cyber incidents…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").

The NCUA should provide examples of non-reportable incidents

While the proposed list of reportable incidents provides a useful starting point for understanding how the rule applies to common types of cyberattacks and malicious events, the NCUA should supplement this list with more examples and also include additional non-reportable incidents. Further, the NCUA should provide more descriptive commentary for the examples of nonreportable incidents that are included in the preamble. For example, understanding whether a cyber incident involves "blocked phishing attempts" or an "unsuccessful malware attack" may involve more complex analysis than the NCUA anticipates. Furthermore, it remains unclear how the agency might regard a phishing email that passes initial email controls where the payload is then blocked, or whether malware installed on a system is deemed an "unsuccessful" attack if it never executes.

While it will be impossible to communicate via regulation every permutation of reportable and nonreportable cyber incidents, NAFCU encourages the NCUA to share more examples with more descriptive background through separate guidance, such as a Letter to Credit Unions, that receives regular updates. Webinars and other forms of educational outreach would also help FICUs better understand the contours of reportable incidents as the cyber threat landscape evolves.

Mechanisms for reporting

The proposed rule does not include any prescribed reporting forms or templates. Instead, the preamble states that a FICU "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." NAFCU supports the proposed accommodation of telephone and email notification channels to facilitate timely response to reportable cyber incidents but recommends the addition of a third channel for reporting incidents such as an online web portal. Additionally, phone and email contacts should be specific individuals rather than general intake points.

The NCUA should also permit credit unions to submit reports to Regional Office contacts or field supervisory teams rather than insist on the use of a centralized hub or platform for general intake. Direct contact with supervisory teams would help facilitate ongoing communication and ensure that NCUA staff evaluating a reportable cyber incident are familiar with the affected credit union's operations. It would also ensure that the impact and severity of an incident is appropriately contextualized based on the field team's understanding of the credit union's IT environment and cyber maturity. Ultimately, a FICU's ability to interact with NCUA staff directly and quickly will better accommodate back and forth communication in situations where initial forensic assessments are fluid.

Harmonization of proposal with existing reporting requirements

The NCUA should clarify how the proposed rule will impact existing reporting for catastrophic acts and events involving unauthorized access to sensitive member information. NAFCU recommends the NCUA seek to harmonize its reporting frameworks in a way that avoids

unnecessary duplication of reports if a particular cyber incident implicates separate reporting regimes.

While Appendix B to Part 748 may provide the agency with notice of some cyber incidents, events involving unauthorized access to sensitive member information are narrower in scope than the full range of reportable events under the proposal. The GLBA notification standard, on which Appendix B is based, does not contemplate the reporting of incidents that disrupt operations or compromise sensitive credit union data but do not compromise sensitive member information. By contrast, all incidents involving unauthorized access to sensitive member information are likely to be considered reportable cyber incidents, in which case a credit union would need to notify the NCUA "as soon as possible" after it determines or reasonably believes that misuse of the information about a member has occurred, and then again within 72-hours under the proposed rule.

NAFCU recommends that the NCUA clarify that the proposed 72-hour period is the controlling timeframe with respect to a cyber incident that involves unauthorized access to sensitive member information, but only when the incident meets the appropriate threshold adopted by the NCUA, be it "material" or "substantial." This would ensure that a single reporting standard exists and eliminate subjective or inconsistent evaluation of a credit union's incident response time under existing Appendix B. Notices to impacted members could then take place as soon as possible after sufficient time allows for a proper investigation and law enforcement activity to take place.

To further avoid confusion that might arise by maintaining multiple reporting standards, the NCUA should also clarify the circumstances under which notice to the NCUA is required for non-cyber incidents that involve unauthorized access to sensitive member information. Appendix B to Part 748 currently focuses on when to notify member but leaves the question of notice to the NCUA more ambiguous.[19] Specifically, the directive to notify the appropriate NCUA Regional Director or State Supervisory Authority (SSA) "as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information" does not clearly convey any limitation on reporting for incidents that are not material.[20] To promote better alignment conceptual alignment between adjacent and potentially overlapping standards (one for certain cyber incidents and another for unauthorized access to sensitive member information), the NCUA should recognize that the materiality of an event and its likelihood to produce substantial harm is the appropriate threshold for agency notification purposes.

Catastrophic act reporting also targets a narrower range of events (a disaster, "natural or otherwise") and is delimited by the definition of vital member services ("informational account inquiries, share withdrawals and deposits, and loan payments and disbursements"). Catastrophic act reporting may not encompass every type of business disruption covered in the reportable cyber incident definition.[21] Some reportable cyber incidents under the proposal could be catastrophic acts causing an interruption in vital member services, in which case the credit union would need to provide both an initial notification, 72 hours after it has determined that a reportable incident

[19] If a credit union "determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible." 12 CFR § 748 Appendix B.
[20] *Id.*
[21] 12 CFR § 748.1(b); § 749.1.

has occurred, a catastrophic act notification within five business days, and then a follow-up report to be filed at the credit union main office within a reasonable period after the event has occurred.

NAFCU asks that the NCUA clarify how cyber incidents governed by both reporting frameworks will be handled, and what information provided in a notice under the proposal will satisfy requirements specific to a catastrophic act report. Given that the initial notification of a catastrophic act is not intended to be as descriptive as the follow-up report described in § 748.1(b), NAFCU recommends clarifying that information provided in response to a reportable cyber incident will also meet the initial reporting requirement for a catastrophic act, and that separate reports will not be required in these instances.

Organizational Improvements

To address overlap between Appendix B to Part 748 and the proposed rule's reporting framework, as well as the introduction of new definitions that may be cross-applicable, the NCUA might consider non-substantive organizational changes to the appendices to consolidate relevant definitions and cybersecurity terminology. The NCUA should aim to organize definitions (e.g., member information, sensitive member information, and the newly defined "sensitive data") in a single list, avoid unnecessary bifurcation of information security program guidelines and incident response standards, and harmonize concepts (e.g., the terms "substantial harm" in Appendix B and "substantial cyber incident") in a way that clearly delineates how these principles will apply to distinct events or elements of an information security program, including when and under what conditions notice to the NCUA is required as touched on above.

Third-party notification

Breach notification provisions in credit union contracts with third party service providers may not fully accommodate the reporting timeline envisioned under the proposal. The proposal notes that 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*" (emphasis added).[22]

Credit union vendor contracts may not specifically address or accommodate access to pre-decisional forensic information that a third party collects when it first learns of a cyber incident. Lack of access to such information could frustrate a credit union's ability to develop an initial report addressing the nature of a cyber incident involving a third-party; it could also delay the time it takes to form a reasonable belief that a reportable cyber incident has occurred.

Third parties may be reluctant to draw conclusions about the scope of a cyber incident and what data is involved until a complete investigation can be performed by their own staff. In these circumstances, a credit union cannot form a reasonable judgment about the scope of the incident

[22] NCUA, "Cyber Incident Notification Requirements for Federally Insured Credit Unions," 87 Fed. Reg. 45029, 45031.

until after the third party has provided its own assessment. If a credit union cannot acquire initial forensic information from a third party before the third party is willing to provide a conclusive statement, and the intervening delay is construed by the NCUA as noncompliant with the proposed notification standard, then credit unions would have limited recourse aside from attempting to renegotiate contracts with their vendors.

NAFCU expects that many smaller credit unions will have significant difficulty modifying contracts with third party service providers—particularly core providers—in the hope of obtaining full access to forensic information and process at the earliest stages. Yet without such access, compliance with the proposed notification requirement is likely to be challenging. Accordingly, NAFCU recommends the NCUA clarify that the time it takes for a credit union to form a reasonable belief about whether a third party has experienced a reportable cyber incident shall appropriately encompass the time taken by the third party to present its own analysis to the credit union. NAFCU also asks that the NCUA consider coordinating with the CFPB to address inequities that may exist in contract negotiations between large core providers and smaller credit unions.

Under the proposed framework, a third party could also unilaterally conclude that a reportable cyber incident occurred and bypass the credit union's procedures for reaching its own determination. While this is less likely to occur, it could also present challenges.

In some situations, a third party's initial investigation of a suspected cyber incident may draw overbroad conclusions about the type of data involved. A resulting decision by the third party to claim, prematurely, that a reportable cyber incident has impacted all clients without regard for variations in individual exposure could result in inconvenience for a credit union client. A third party serving many customers might find it advantageous from a risk management perspective to unilaterally classify a cyber incident as reportable if there are not enough resources to perform client-specific forensic work to uncover the exact contours of a compromise or other event. In these circumstances, a credit union client that is not, in fact, exposed to a third-party cyber incident could nevertheless suffer reputational injury and the inconvenience of additional supervisory attention resulting from the third party's premature conclusion that a cyber incident is reportable when it is not.

To avoid conflicting or premature conclusions in these circumstances, NAFCU recommends the NCUA recognize that a credit union will have final say with respect to the question of whether a reportable cyber incident has occurred. NAFCU believes that deference to credit union judgement in this domain would not compromise the overall purpose of the rule.

NAFCU also asks that the NCUA avoid imposing a third-party notification requirement when a credit union employee's personally identifiable information is implicated in a data breach of a third-party that has no affiliation or agreement with the credit union.[23] Part 748 is primarily concerned with establishing technical safeguards to ensure the availability, integrity and confidentiality of credit union information systems, including credit union systems operated by third parties.

[23] While not explicitly incorporated in proposed 748.1(c), events involving an employee's PII are referenced in the preamble's example list of reportable incidents.

Expanding Part 748 compliance to encompass systems that are not operated or controlled by credit unions, such as healthcare providers, would represent a significant expansion of the NCUA's authority under the GLBA and detract from the core mission of supporting *credit union* cybersecurity. While the compromise of a third-party holding a credit union employee's PII can create vulnerability, these unaffiliated parties will have their own cyber incident reporting obligations under the CIRCIA. Accordingly, a better way for the NCUA to gather information about cyber incidents that do not directly implicate FICUs or their service providers is to develop strong information sharing capabilities and effective coordination with CISA and Treasury—agencies that are the practical nerve centers for synthesizing cyber intelligence and events that occur outside the financial sector.

Industry reliance on NCUA data security standards depends upon regulatory coordination and recognition of jurisdictional boundaries

On August 11, 2022, the Consumer Financial Protection Bureau (CFPB or Bureau) issued a circular stating that financial companies may violate federal consumer financial protection law when they fail to safeguard consumer data.[24] The Circular indicates that failure to meet certain minimum data or cybersecurity safeguards might constitute an unfair act or practice.

The CFPB's attempt to leverage its unfair, deceptive, and abusive acts and practices (UDAAP) authority to promulgate data security standards through circulars represents a significant expansion of its rulemaking and enforcement jurisdiction—at least with respect to FICUs. While NAFCU anticipates that the circular will have greater practical significance for nonbank covered persons subject to the CFPB's supervisory jurisdiction, it remains unclear how CFPB examiners might apply the circular to federally insured institutions that already have a prudential regulator.

Separately, the CFPB's publication of CMS-IT examination procedures signals that the agency may be inclined to assess the adequacy of data security safeguards through the lens of UDAAP for all covered persons.[25] However, the NCUA has exclusive rulemaking authority to implement technical and administrative safeguards for FICUs under the GLBA. To preserve the NCUA's role as the industry's primary functional regulator, and avoid the potential for conflicting supervisory expectations, NAFCU asks that the NCUA ensure that appropriate coordination exists with the CFPB and that credit unions will be examined for data security compliance based on the standards and expectations communicated in Part 748 of NCUA's regulations.

Confidentiality of Reports

The NCUA has clarified in the proposal that any information provided by a FICU related to a cyber incident, would be subject to the NCUA's confidentiality rules. While NAFCU appreciates this

[24] *See* CFPB, Consumer Financial Protection Circular 2022-04 (August 11, 2022), *available at* https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.
[25] *See* CFPB, Compliance management review – information technology examination procedures, (September 20, 2021), available at https://www.consumerfinance.gov/compliance/supervision-examinations/compliance-management-review-information-technology-examination-procedures/.

statement in the preamble, NAFCU asks that the NCUA include a clear statement in the regulatory text that notices and reports to the NCUA related to cyber incidents are not only subject to the rules in Part 729, but also exempt from Freedom of Information Act (FOIA) requests. Such a statement would clearly communicate the applicability of the relevant statutory FOIA exemption and give credit unions greater confidence that sensitive information about IT systems or operations will not be inadvertently disclosed to the public.[26]

Conclusion

NAFCU and its members appreciate the opportunity to comment on the NCUA's proposed rule. Should you have any questions or require any additional information, please contact me at amorris@nafcu.org or (703) 842-2266.

Sincerely,

Andrew Morris
Senior Counsel for Research and Policy

[26] *See* 5 U.S.C. § 552(b)(8) (2000) (describing FOIA exemption for records "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions")