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

October 31, 2023

Kemba E. Walden
Acting National Cyber Director
Office of the National Cyber Director
1800 F Street, N.W.
Washington, D.C. 20405

RE: Request for Information on Cyber Regulatory Harmonization (RIN: 0301-AA00)

Dear Director Walden:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response to the Office of the National Cyber Director's Request for Information on cyber regulatory harmonization. NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve 138 million consumers with personal and small business financial services products. NAFCU supports harmonization of cybersecurity regulations to reduce inconsistency and administrative burden for federally insured credit unions (FICUs). Credit unions can encounter numerous variations of cybersecurity rules depending on where they operate, as many states have adopted their own, unique rules for information security programs. While all FICUs are examined for cybersecurity compliance by the National Credit Union Administration (NCUA), and are expected to follow the NCUA's data security and incident response rules, the Consumer Financial Protection Bureau (CFPB) has also asserted that it has supervisory and enforcement powers in the domain of cybersecurity—a position that is questionable from a legal perspective and detrimental to efficient administration of the Gramm-Leach Bliley's Act's (GLBA) information safeguards requirements.

State Laws

FICUs operating in states with unique rules for information security programs may confront standards that do not align with the expectations of the NCUA, which has adopted its own rules for FICUs.

Massachusetts, for example, requires persons who own or license personal information about a resident of the state to adopt specific safeguards for protecting personal information. One of those safeguards includes a program for "[i]mposing disciplinary measures for violations of the comprehensive information security program rules."[1] No equivalent disciplinary component is found in Part 748 of the NCUA's rules implementing the GLBA's safeguards provisions.

For financial institutions operating under a license or charter in New York, the New York Department of Financial Services (NYDFS) requires compliance with detailed cybersecurity rules that provide, among other things, granular qualifications for cybersecurity personnel. NYDFS regulations state that covered entities must utilize qualified cybersecurity personnel that meet continuous learning requirements.[2]

[1] 200 CMR 17.03(d).
[2] *See* 23 NYCRR 500.10

NCUA rules do not limit the type of personnel who may satisfy a FICU's compliance with information security program requirements.[3]

State laws also encompass unique incident reporting requirements that can impede efficient response to cyber events, particularly in cases where different deadlines and notice requirements apply. While the request for information does not invite comment on harmonization of cyber incident reporting rules, it is worth noting that differences exist between some states and these differences can contribute to administrative burden. Highly detailed forensic assessments of cyber incidents are not always practical in the immediate aftermath of a cyber event and notices that require such information can distract from remediation activities.

NAFCU recommends the ONCD catalogue differences in state information security requirements for financial institutions that create conflict or inconsistency with the guidelines and standards adopted by federal banking regulators, such as the NCUA. Analysis of discrepancies between state and federal law may help financial regulatory agencies engage in productive dialogue around cyber regulatory harmonization. It could also serve as a compliance aid for small financial institutions.

Overlapping Federal Cybersecurity Standards

The NCUA is the primary regulator for federal credit unions and has developed information security rules applicable to all FICUs. Part 748 of the NCUA's regulations implements section 501(b) of the GLBA.[4] Sections 504(a) and 505(a)(2) establish the NCUA's exclusive rulemaking and enforcement jurisdiction over credit unions with respect to the GLBA's safeguards provisions.[5] Section 1002(12)(J) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), however, excludes financial institutions' information security safeguards under GLBA section 501(b) from the CFPB's rulemaking, examination, and enforcement authority.[6]

Despite the GLBA's clear assignment of information security responsibilities to the NCUA with respect to FICUs, the Consumer Financial Protection Bureau (CFPB) has asserted that it also possesses the authority to create and enforce cybersecurity rules for covered persons under the Dodd-Frank Act.[7] However, the basis for this authority is questionable and does not derive from any specific provision of the Dodd-Frank Act. Instead, the CFPB broadly interprets the Dodd-Frank Act's prohibition on unfair, deceptive and abusive acts and practices (UDAAP) to give the agency the necessary power to develop its own cybersecurity standards for financial institutions—even those for which the GLBA has designated a specific, federal banking agency (e.g., the NCUA, FDIC, or OCC) to administer information safeguard requirements. The CFPB believes that if IT violations can result in consumer harm or violations of consumer financial law, there is a sufficient jurisdictional nexus to assert rulemaking and enforcement authority in the IT security domain.

[3] *See* 12 CFR Part 748 Appendix A
[4] *See* 12 U.S.C. § 6801(b).
[5] *See* 12 U.S.C. §§ 6804(a) and 6805(a)(2).
[6] 12 U.S.C. § 5481(12)(J)
[7] 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/.

The CFPB's involvement in cybersecurity regulation has created a parallel set of standards for FICUs. Moreover, the CFPB's approach to cybersecurity differs from the traditional emphasis on safety and soundness that guides the functional banking regulators.

The CFPB frames its authority and purpose for implementing cybersecurity rules in terms of preventing violations of consumer financial law. This fundamental difference in perspective may not always be complementary to risk-based cybersecurity principles and likely deviates from the intent of Congress in the GLBA to administer technical safeguards through the functional banking regulators.[8]

For example, the CFPB's IT examination procedures instruct examiners to collect and review IT-related consumer complaints, which may have little bearing on the actual security of IT systems. These reviews could distract from core security activities by demanding review of performance or user-experience factors.[9] CFPB examiners are also instructed to review whether a financial institution's IT personnel are trained to understand compliance requirements under federal consumer financial law, including prohibitions on UDAAP.[10] Dividing the attention of IT professionals by demanding training in consumer financial law—as opposed to the data security requirements prescribed by a functional federal regulator designated by the GLBA—also risks impairing the efficacy of IT security programs.

While the CFPB's adoption of IT examination procedures and data security requirements may have the benefit of addressing supervisory gaps in the financial sector (unlike FICUs, certain nonbank entities are not regularly examined for cybersecurity compliance), they are counterproductive when applied to credit unions already supervised by the NCUA. Accordingly, NAFCU encourages the ONCD to examine the effect of the CFPB's decision to promulgate cybersecurity standards for institutions already subject to regular cyber examination through their respective federal banking regulators, such as FICUs.

The ONCD should also promote interagency dialogue between the CFPB and the NCUA to ensure that the latter's exclusive rulemaking and enforcement powers under the GLBA are not undermined by parallel standards or fundamentally different supervisory expectations.

Conclusion

NAFCU appreciates the ONCD's interest in supporting cyber regulatory harmonization and identifying areas where different standards may create conflict, confusion, or duplication of effort. If you have any questions or concerns, please do not hesitate to contact me at amorris@nafcu.org or (703) 842-2266.

[8] *Compare* National Institute of Standards and Technology, Initial Public Draft of Cybersecurity Framework 2.0, 8 (August 8, 2023) ("Organizations may choose to handle risk in different ways — including mitigating, transferring, avoiding, *or accepting the risks* — depending on the potential impacts") (emphasis added) *with* CFPB, Data Security Circular 2022-04, 3 (August 11, 2022) ("The CFPB is unaware of any instance in which a court applying an unfairness standard has found that the substantial injury caused or likely to have been caused by a company's poor data security practices was outweighed by countervailing benefits to consumers or competition").
[9] *See* CFPB, Compliance Management Review – IT, 13-14 (September 2021), available at https://files.consumerfinance.gov/f/documents/cfpb_compliance-management-review-information-technology_examination-procedures.pdf
[10] *See id*. at 9.

Sincerely,

Andrew Morris
Senior Counsel for Research and Policy