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

August 2, 2019

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, D.C. 20580

RE: Safeguards Rule, 16 CFR part 314, Project No. 145407

Dear Sir or Madam:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only national trade association focusing exclusively on federal issues affecting the nation's federally insured credit unions, I am writing in regard to the Federal Trade Commission's (FTC) proposed amendments to its Safeguards Rule, which implements Subtitle A of Title V of the *Gramm-Leach-Blilely Act* (GLBA). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 117 million consumers with personal and small business financial service products. In general, NAFCU supports the intent of the proposal, which aligns data security standards for covered financial companies more closely with those already established by prudential regulators.

General Comments

Modernization of the Safeguards Rule is desirable in an environment where nonbank financial companies handle large amounts of consumer data but may not be subject to the same degree of regular examination or formal supervision as credit unions and other insured depositories. Although federally-insured credit unions are not subject to the FTC's Safeguards Rule, they follow regulations and guidance promulgated by the National Credit Union Administration (NCUA) and the Federal Financial Institutions Examination Council (FFIEC). Given the severity and extent of recent data breaches at financial companies subject to the FTC's jurisdiction and the Safeguards Rule, such as Equifax, it is imperative to adopt more comprehensive security requirements.

The proposed incident response plan represents an improvement in terms of cyber hygiene, but we recommend that that the FTC consider additional reporting and notification requirements to ensure that security breaches can be contained and mitigated as quickly as possible. Because the FTC lacks the supervisory authority to examine covered financial companies for compliance with the Safeguards Rule, and may only take enforcement action after the fact, a notice requirement provides an appropriate incentive for covered financial companies to disclose information to consumers and relevant regulatory bodies. Required disclosure to regulators is particularly important to ensure independent assessment of whether a security incident represents a threat to

consumer privacy or a contagion to other financial institutions. NAFCU considers mandatory reporting and disclosure essential in any federal data security standard and has, for many years, advocated for legislation that would hold merchants and other entities handling financial information accountable for the consequences of data breaches.

NAFCU also recommends that the FTC clarify that a federally-insured credit union's "subsidiary" includes a credit union service organization (CUSO). Doing so would ensure that CUSOs are not subject to duplicative rules originating from different agencies.

Part 748 of the NCUA's regulations implements section 501(b) of the GLBA and contains a more extensive set of security program guidelines than what the FTC requires under its equivalent rule today. CUSOs, which are organizations that primarily serve credit unions or their members, abide by NCUA rules to harmonize operations with their credit union owners.[1] The NCUA may also perform CUSO reviews as part of a credit union exam or as a standalone evaluation. In both cases, the examiner could require the CUSO to produce information related to its data processing systems, internal controls, and intrusion detection and monitoring procedures.[2] Furthermore, CUSOs that handle credit union member information must adopt a security program that meets the owner credit union's compliance standards because all federally-insured credit unions must secure contractual promises from affiliated third party service providers to protect the confidentiality and security of member information.[3] For CUSOs owned by corporate credit unions, the NCUA may require explicit compliance with Part 748 security program requirements depending on the complexity of the CUSO's activities.[4] In this context, the proposed amendments to the Safeguards Rule could disrupt existing arrangements by requiring CUSOs to follow FTC standards rather than what they are most familiar with, which are the credit union specific security guidelines contained in Part 748 of the NCUA's regulations.

The scope of the current Safeguards Rule is set forth in 16 CFR § 314.1(b), which provides that the rule applies to those "financial institutions" over which the FTC has jurisdiction. The proposal would clarify this statement by further specifying that the term jurisdiction encompasses the FTC's rulemaking and enforcement authorities. As noted in the proposal, entities subject to the Safeguards Rule are covered as a result of the agency's enforcement jurisdiction rather than its rulemaking jurisdiction.

In general, covered financial institutions subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the GLBA.[5] Section 505(a)(2) of the GLBA specifically excludes federally-insured credit

[1] See 12 CFR § 741.222(a).
[2] See National Credit Union Administration, National Supervision Policy Manual, 139 (last updated July 31, 2018). See also, National Credit Union Administration, Examiner's Guide, CUSOs – Stand-Alone Reviews, available at https://publishedguides.ncua.gov/examiner/Pages/Content/ExaminersGuide/CUSOs/CUSO_Reviews/Stand-Alone.htm.
[3] *See* 12 CFR § 748 -- Appendix A.
[4] See National Credit Union Administration, Approved Corporate CUSO Activities, available at https://www.ncua.gov/regulation-supervision/corporate-credit-unions/corporate-cuso-activities/approved-corporate-cuso-activities.
[5] See 15 U.S.C. § 6805(a).

unions and their subsidiaries from the FTC's enforcement authority; however, the meaning of subsidiary is not expressly defined in this subsection. Instead, Section 505(d) of the GLBA provides that terms used in subsection (a)(1) (which is not applicable to federally-insured credit unions), and not otherwise defined in 12 U.S.C § 1813(s), shall have the same meaning as given in 12 U.S.C. § 3101.[6]

The term subsidiary does not appear in 12 U.S.C. § 1813(s). However, 12 U.S.C. § 3101(13) provides that the term "subsidiary" shall have the same meanings as assigned in the *Bank Holding Company Act of 1956* (BHCA) (12 U.S.C. § 1841, et seq.). The BHCA defines subsidiary only with respect to a bank holding companies and does not address the relationship that exists between federally-insured credit unions and CUSOs. Furthermore, the concept of control articulated in the BHCA is not responsive to the unique characteristics of CUSOs, which in all cases are practically controlled by credit unions even if no single credit union owner has a majority interest. This is because CUSOs, by definition, must be engaged primarily in providing products or services to credit unions or credit union members.[7] To account for the unique structure of these organizations and avoid confusion, CUSOs should be explicitly designated as subsidiaries of federally-insured credit unions.

Conclusion

On behalf of this country's credit unions, owned by 117 million members, NAFCU appreciates the opportunity to provide comments on the proposed changes to the FTC's Safeguards Rule. We recommend that the FTC clarify that CUSOs are subsidiaries of federally-insured credit unions, which would allow these organizations to focus on what they are most familiar with: the security guidelines contained in Part 748 of the NCUA's regulations. Should you have any questions or concerns, please do not hesitate to contact me at amorris@nafcu.org or 703-842-2266.

Sincerely,

Andrew Morris
Senior Counsel for Research and Policy

[6] See 15 U.S.C. § 6805(d).
[7] See 12 CFR § 712.1(d).