Credit Union National Association
CUNA

WASHINGTON, D.C.

99 M Street SE
Suite 300
Washington, D.C. 20003-3799

Phone: 202-638-5777
Fax: 202-638-7734

August 1, 2019

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC–5610 (Annex B)
Washington, DC 20580

Re: Safeguards Rule, 16 CFR part 314, Project No. P145407

Dear Commission Secretary:

The Credit Union National Association (CUNA) appreciates the opportunity to submit comments to the Federal Trade Commission (the "FTC") in response to the request for comment regarding potential modifications the Safeguards Rule. CUNA represents America's credit unions and their 115 million members. There are 115 privately insured credit unions and unlike the approximately 5,300 federally insured credit unions, they are subject to the requirements in the FTC's Safeguards Rule.

CUNA's top legislative priority is for Congress to pass a federal privacy bill that includes a national data security standard that regulates entities based on the type of data that they handle or maintain. CUNA members believe there is an urgent need for strong federal data security and privacy laws that protect all data from theft and misuse by entities and individuals that handle and maintain personal data either directly or indirectly. All federally insured credit unions and banks comply with data security and privacy requirements set forth in the Gramm Leach Bliley Act ("GLBA"), and are examined by federal and state regulators for compliance. We believe that all American business entities and individuals that handle or maintain consumers' personal information should be subject to similar requirements.

We know there is trepidation in placing data security and privacy requirements on small businesses. Credit unions are the example of how this can be accomplished. The size of federally insured credit unions varies from less than 210 members with fewer than $20,000 in assets and volunteer employees to over 8,400,000 members with over $100 billion in assets. As mentioned above, federally insured credit unions are subject to the National Credit Union Administration's ('NCUA") data security and privacy regulations, which implement GLBA's requirements. These regulations are flexible enough that both volunteer employees and sophisticated information technology staff can apply the requirements to their respective credit unions. We do not believe that GLBA is perfect, and clearly more work must be done to incorporate all businesses into a single national standard.

Unfortunately, the mere existence of data and privacy laws do not ensure total protection of data from nefarious actors. Even sophisticated financial institutions have suffered incidents where large amounts

of data have been stolen. However, most of the large data breaches from financial institutions and others such as Marriott, Home Depot and Target could have been prevented with more vigilant information security practices. We believe that federal data security laws with federal enforcement authority would have forced these negligent actors to take their duty to protect customers' information more seriously.

Strong data security laws will not stop criminals or rogue nation states from attempting to penetrate even the most sophisticated data and cybersecurity defenses; however, American consumers that trust their personal information to businesses deserve the most diligent effort by those businesses and entities to protect this data from theft and misuse. And absent stringent federal requirements, it's clear that many businesses will not devote the necessary resources to protecting consumers' information.

We realize that passing new legislation requires action by Congress and is beyond the scope of this Request for Comment and the FTC's statutory authority; nonetheless, the FTC is in the position to help lead the effort for robust protection for all consumers.

Exceptions – Section 314.6

There are 115 privately insured credit unions that are subject to the Safeguards Rule. Not only are these credit unions required to comply with the regulation's requirements, they are examined by state regulators in the state in which they are chartered for compliance. This is an extra level of protection that most other entities subject to the Safeguards Rule do not have. Because privately insured credit unions are examined by state examiners who are likely more familiar with NCUA's data security regulation or their own state's data security regulation, the FTC should explore allowing a privately insured credit union to comply with either NCUA's regulation or the regulation of the state in which the credit union is chartered. This would simplify compliance while still protecting privately insured credit union members' information.

The proposed rule is too prescriptive for most credit unions but the exemptions in Section 314.6 will help the 55 privately insured credit unions with fewer than 5,000 members comply. These credit unions will not have to comply with the requirements to: (1) perform a written risk assessment; (2) conduct continuous monitoring or annual penetration testing and a biannual vulnerability assessment; (3) prepare a written incident response plan; or (4) prepare an annual written report by the Chief Information Security Officer (CISO). Instead of creating an overly prescriptive rule with an exemption for small entity or individual compliance, we suggest that a rule be commensurate with the sensitivity of the information possessed and the complexity and scope of the activities of an individual or entity; thus risk-based.

Incident Response Plan

We support proposed paragraph (h)'s requirements that financial institutions establish an incident response plan. This is required by NCUA for credit unions. An incident response plan helps ensure that an entity is prepared in case of an incident by planning how it will respond and what is required for the response. We also support a notification requirement as part of the incident response plan. The notification requirement should include FTC and consumer notification requirements.

Conclusion

Enhanced data security requirements should help safeguard consumers' private information. We generally support FTC's amendments to the Safeguards Rule; although, as shown from our comments above we think that the definition of financial institution should be broadened as much as possible to maximize consumer protection. Unfortunately, more needs to be done so that data is properly secured no matter what type of entity possesses it. It is for this reason that CUNA and our members believe Americans' privacy will not have the protection Americans deserve until Congress passes a law with both strong privacy and data security protections that regulates based on the type of information handled or maintained.

If you have questions or would like to discuss our comments further, please do not hesitate to contact me at (202) 508-6705.

Sincerely,

Lance Noggle
Senior Director of Advocacy & Senior Counsel for Payments & Cybersecurity