Credit Union National Association
CUNA

Washington, D.C.
99 M Street SE, Suite 300
Washington, D.C. 20003-3799
Phone: 202-638-5777
Toll-Free: 800-356-9655

November 21, 2022

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

Re: Commercial Surveillance ANPR, R111004

To Whom It May Concern:

On behalf of America's credit unions, I am writing to the Federal Trade Commission (FTC) in response to the advanced notice of proposed rulemaking on commercial surveillance and data security (ANPR).[1] The Credit Union National Association (CUNA) represents America's credit unions and their 130 million members.

General Comments

Credit unions strongly support the enactment of a comprehensive national data security and data privacy standard that includes robust security requirements that apply to all who collect or hold personal data and is preemptive of state laws. We firmly believe there can be no data privacy until there is data security. Securing and protecting consumer data is important not only for consumers' individual financial health but as a further safeguard against rogue international agents and interference by foreign governments.

Data privacy and data security are major concerns for Americans given the frequency of reports of misuse of personally identifiable information (PII) data by businesses and breaches by criminal actors, some of which are state sponsored. Since 2005, there have been more than 10,000 data breaches—exposing nearly 12 billion consumer records. These breaches have cost credit unions, banks, and the consumers they serve hundreds of millions of dollars, and they have compromised the consumers' privacy, jeopardizing their financial security.

Mitigating losses from merchant data breaches remains a top credit union priority. Data breaches that expose card information and consumers' personally identifiable information, such as what happened with the 2017 Equifax data breach, cost credit unions and their member-owners enormous sums of money. Additionally, this breach gave criminals copious amounts of personal information which could be used to directly defraud credit unions and other financial institutions. Even though financial institutions have an affirmative duty to make consumers whole for losses

[1] Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (August 22, 2022), *available at* https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf.

incurred from data breaches resulting in fraud on their accounts, the repercussions for both the financial institution and the consumer are substantial.

Losses to credit unions from merchant data breaches impact credit union members in multiple ways. Even though credit unions bear the direct financial losses of fraud resulting from a merchant data breach, members also bear a cost as owners of credit unions because credit unions are member-owned organizations. Technically, members are shareholders but in the cooperative sense, which means that every credit union member is an equal owner who shares in the success of a credit union by receiving lower interest rates on loans, higher interest rates on deposit products, and lower fees. Due to credit unions' ownership structure, any loss to a credit union from a data breach impacts members directly as their member benefits are directly decreased by losses from the breaches. These losses can be exacerbated by credit unions' membership requirements that can create concentrations of memberships and lead to a more impactful data breach.

Existing Data Security and Privacy Framework Under GLBA Should Exempt Credit Unions from Duplicative Rulemaking

Stringent information security and privacy practices have long been part of credit unions' business practices and are necessary as financial institutions are entrusted with consumers' personal information. This responsibility is reflected in the strong information security and privacy regime that governs data practices for the financial services industry as set forth in the Gramm Leach Bliley Act (GLBA). GLBA's protection requirements are strengthened by federal and state regulators' examinations for compliance with GLBA's requirements and robust enforcement for violations. Several of these significant regulatory requirements and internal safeguards include:

- Federal Requirements to Protect Information: Title V of the GLBA and its implementing rules and regulations require credit unions to protect the security, integrity, and confidentiality of consumer information.
- Federal Requirements to Notify Consumers: Credit unions are required to notify their members whenever there is a data breach where the misuse of member information has occurred or where it is reasonably likely that misuse will occur.
- Strong Federal Oversight and Examination: Under their broad-based statutory supervisory and examination authority, the National Credit Union Administration and the Consumer Financial Protection Bureau regularly examine credit unions for compliance with data protection, privacy, and notice requirements.
- Strong Federal Sanction Authority: Under numerous provisions of federal law, credit unions are subject to substantial sanctions and monetary penalties for failure to comply with statutory and regulatory requirements.

This extensive legal, regulatory examination and enforcement framework ensures that credit unions robustly protect consumers' personal financial information and makes clear that credit unions, and the broader financial services industry, should be exempt from this FTC rulemaking. Financial institutions comply with a rigorous, comprehensive data security and privacy framework and, in fact, compliance is an element of fundamental safety and soundness for the overall banking system. Additionally, it must not be overlooked that the financial industry is the only sector subject to ongoing examination to ensure compliance with these security and privacy standards.

The ANPR cites "laws and regulations" enacted by several states "impos[ing] restrictions on companies' collection, use, analysis, retention, transfer, sharing, and sale or other monetization of consumer data" as evidence of the need for this rulemaking. It is imperative that the FTC acknowledge that most state privacy laws include an entity level GLBA exemption—an avoidance of duplicative requirements and a recognition of the effective consumer protections provided by GLBA. The FTC should follow this lead and include an entity level GLBA exemption in its rulemaking.

While considering the feasibility of its rulemaking, the FTC should look to small financial institutions' experience with the GLBA data security and privacy standards. Financial institutions range in size from banks with over $2 trillion in assets to credit unions with less than $1 million in assets and not even a single full-time employee. Financial institutions of all sizes are subject to the same standards under GLBA, including strict regulatory oversight by federal and state regulators. This experience with GLBA requirements demonstrates that even the smallest merchant or business can meet reasonable data security and privacy requirements based on risk, which is not necessarily tied to the size of a merchant but more to the PII that could be lost.

With this in mind, we urge the FTC's consideration of our data security and privacy principles:

Data Privacy and Data Security are Hand in Glove:
Any new comprehensive regulatory framework should include both data privacy and data security standards. Simply put, data cannot be kept private unless it is also secured.

Everyone Should Follow the Same Rules:
The new rule should encompass all businesses, institutions, and organizations by raising expectations for these other sectors up to a standard very similar to that currently in place for financial institutions under GLBA.

Breach Disclosure and Consumer Notification Are Important, but These Requirements Alone Will Not Enhance Security or Privacy:
Breach notification or disclosure requirements are important, but they are akin to sounding the alarm after the fire has burned down the building. By the time a breach is disclosed, harm could already have befallen hundreds or thousands, if not millions, of individuals.

Hold Entities that Jeopardize Consumer Privacy and Security Accountable Through Private Right of Action and Regulatory Enforcement:
The rule should provide mechanisms to address the harm that results from violations, including data breach. Increasingly, courts are recognizing rights of action for individuals and companies (including credit unions); however, individuals and companies should be afforded a private right of action to hold those that violate the law accountable, and regulators should have the ability to act against entities that violate the law.

Recognize This Issue for What it is—A National Security Issue:
More and more, data breaches that expose consumer PII are perpetrated by foreign governments and other rogue international entities. The proceeds from these attacks are

being used to fund illicit activity. The nature of these breaches alone calls for a strong federal response that ensures all involved in collecting, holding, and using PII do so with the security of the information as the paramount concern.

Conclusion

Credit unions support a strong data security standard with clear, robust enforcement mechanisms like those already in place for financial institutions under the GLBA and other financial data security and privacy laws. CUNA encourages the FTC to avoid confusion and duplicative requirements by including an entity-level GLBA exemption in its rulemaking.

If you have questions about our comments, please do not hesitate to contact me at (202) 577-3463.

Sincerely,

Madison Rose
Director of Advocacy & Counsel for Payments and Technology