



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 20, 2021

The Honorable Stephen Lynch
Chairman
Task Force on Financial Technology
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

The Honorable Warren Davidson
Ranking Member
Task Force on Financial Technology
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing, "Preserving the Right of Consumers to Access Personal Financial Data"

Dear Chairman Lynch and Ranking Member Davidson:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) ahead of tomorrow's hearing on "Preserving the Right of Consumers to Access Personal Financial Data." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 127 million consumers with personal and small business financial service products. NAFCU and our members welcome the Task Force's examination of the use of consumers' data.

As NAFCU shared with the Financial Services Committee back in March, fintech companies that specialize in lending, payments, or data aggregation present unique consumer protection concerns. A fintech company that permits consumers to consolidate control over multiple accounts on a single platform elevates the risk of fraud and may not be subject to regular cybersecurity examination and data privacy and protection requirements in the same way that credit unions are under the *Gramm-Leach-Bliley Act* (GLBA). Although non-bank lenders are subject to consumer protection rules, the connectivity and segregation of discrete services within the fintech marketplace can create supervisory challenges.

These concerns have come to light recently as the Consumer Financial Protection Bureau (CFPB) addresses issues related to errors under the *Electronic Fund Transfer Act* (Regulation E). Credit unions continue to face error resolution challenges, particularly when a transaction involves a mobile payment application. Third party access to a consumer's personal financial data, often via a fintech platform, can lead to disputed transactions. As mobile payment applications from fintechs have become more prevalent during the pandemic, credit unions have seen an increase in fraud related to the use of these applications. That is why NAFCU believes Congress should amend certain portions of the *Electronic Fund Transfer Act* and direct the CFPB to issue updates to Regulation E to clarify that fintech providers should hold some responsibility for resolving errors and disputed transactions involving electronic transfers from consumer accounts made using their platforms.

We also continue to believe there is an urgent need for a national data security standard for all of those that collect and store consumer information. Intertwined with data security is data privacy and the need to protect consumer information. In 2019, recognizing the importance of data privacy and the ongoing privacy debate, NAFCU issued a series of data privacy principles that call for a comprehensive federal data privacy standard that protects consumers, harmonizes existing federal data privacy laws, and preempts state privacy laws. As the Task Force works to achieve a path forward on the collection of financial data, NAFCU recommends you include the following elements as key aspects in any such proposal:

- **A comprehensive national data security standard covering all entities that collect and store consumer information.** In order to protect consumers, retailers, fintech companies, and any other organizations handling personal information should be required to provide reliable and secure information systems similar to those required of credit unions.
- **Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.** The patchwork of federal and state privacy laws creates an environment where consumers receive multiple disclosures on different information and their rights vary significantly across different types of organizations; this situation is confusing for consumers, burdensome for credit unions, and can only be resolved by a federal law that preempts state laws.
- **Delegation of enforcement authority to the appropriate sectoral regulator.** For credit unions, the National Credit Union Administration (NCUA) should be the sole regulator. Allowing the NCUA, which is well versed in the unique nature of credit unions and their operations, to continue to examine and enforce any privacy and cybersecurity requirements is the most efficient option for both credit unions and American taxpayers.
- **A safe harbor for businesses that take reasonable measures to comply with the privacy standards.** Any federal data privacy bill should provide for principles-based requirements based on an organization's specific operations and risk profile, and a safe harbor for organizations that design and implement appropriate measures.
- **Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.** Providing multiple privacy disclosures and opt-out mechanisms across multiple channels creates confusion for

The Honorable Stephen Lynch
The Honorable Warren Davidson
September 20, 2021
Page 3 of 3

consumers and unreasonable burdens for credit unions. A new privacy law should incorporate the GLBA's requirements to avoid conflicting or duplicative disclosure requirements.

- **Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.** Actual damages to consumers are too difficult to establish by evidence and statutory damages for violations are incredibly ripe for frivolous lawsuits; sectoral regulators should have the power to assess scalable civil penalties, which can then be used to remedy and prevent consumer harm in a meaningful way.

NAFCU looks forward to working with the Task Force and those in industry to address these concerns with consumer privacy and data security. In particular, any federal privacy legislation must be operationally workable for small- and medium-sized businesses like credit unions. We would urge you to work collaboratively with other interested Committees in the House to find a package that can advance and receive bipartisan support.

On behalf of our nation's credit unions and their more than 127 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information, please contact me or Janelle Relfe, NAFCU's Associate Director of Legislative Affairs, at 703-842-2836 or jrelfe@nafcu.org.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the House Financial Services Committee Task Force on Financial Technology