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

November 2, 2021

The Honorable Ed Perlmutter
Chairman
Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

The Honorable Blaine Luetkemeyer
Ranking Member
Subcommittee on Consumer Protection and Financial Institutions
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

Re: Tomorrow's Hearing on "Cyber Threats, Consumer Data, and the Financial System"

Dear Chairman Perlmutter and Ranking Member Luetkemeyer:

I am writing on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) to share our thoughts ahead of tomorrow's hearing, "Cyber Threats, Consumer Data, and the Financial System." 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 thanks the Subcommittee for holding this important hearing, and we appreciate the opportunity to share the perspective of our credit unions.

NAFCU's Privacy Concerns with Proposed IRS Reporting Requirements

Any discussion on consumer privacy must start with NAFCU reiterating our strong opposition to the provision in the fiscal year 2022 (FY 2022) Budget Resolution that proposes a new reporting requirement on financial institutions for account inflow and outflow information of American taxpayers to the Internal Revenue Service (IRS) for accounts with over $10,000 in transactions annually. We strongly urge Congress to not include any language enacting this provision in the *Build Back Better Act* and are pleased to see it not included in the draft text released last week.

This provision would be an invasion of privacy into countless Americans' daily lives. Financial institutions already face a robust reporting regime for financial transactions, such as 1099s, Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs). At any threshold, requiring credit unions to report on gross inflows and outflows of accounts poses regulatory costs and challenges while threatening to reduce participation in financial services and invade the privacy of hundreds of millions. While we support efforts to increase taxpayer compliance, we do not believe adding untested reporting requirements to an already heavily regulated industry is the answer. Instead, we would encourage Congress and the Administration to seek better solutions for taxpayer compliance, such as increased funding and support for IRS improvements. We remain committed to working with you in that effort.

NAFCU Opposes Granting NCUA Additional Authority Over Vendors

NAFCU continues to remain opposed to the legislative proposal under consideration by the Subcommittee, the *Strengthening Cybersecurity for the Financial Sector Act*. NAFCU and our member credit unions believe that cybersecurity, including the security of vendors that credit unions do business with, is an important issue. However, we are opposed to granting additional authority to the National Credit Union Administration (NCUA) to examine third parties at this time. NAFCU believes in a strong NCUA, but we also believe that the NCUA should stay focused on where their expertise lies—regulating credit unions. Credit unions fund the NCUA budget. Implementing such new authority for the NCUA would require significant expenditures by the agency. The history of the NCUA's budget growth has shown that these costs would ultimately be borne by credit unions and their members.

There are other tools already in place for the agency to get access to information about vendors. We believe the agency's time and resources are better focused on reducing regulatory burden by coordinating efforts among the financial regulators. The NCUA sits on the Federal Financial Institutions Examination Council (FFIEC) with the Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC), and the Federal Reserve. The FFIEC was created to coordinate examination findings and approach in the name of consistency and to avoid duplication. This means that as a member of the FFIEC, the NCUA should be able to request the results of an examination of a core processor from the other regulators and not have to send another exam team from the NCUA into their business and duplicate an examination. This would seem to be an unnecessary burden on these small businesses. Additionally, if the NCUA did its own examination, the likelihood of finding anything the other regulators did not would seem to be close to nil.

Instead of granting the NCUA vendor examination authority, Congress should encourage the agency to use the FFIEC and gain access to the information on exam findings on companies that have already been examined by other regulators. This would address the NCUA's concerns without creating additional costs to credit unions and increasing regulatory burdens on credit unions and small businesses.

NAFCU Supports a National Data Security Standard

As NAFCU has previously communicated to Congress, there is an urgent need for a national data security standard for entities that collect and store consumers' personal and financial information that are not already subject to the same stringent requirements as depository institutions. Unfortunately, retailers and fintechs are not held to the same data security expectations as depository institutions, which have faced rigorous cybersecurity exams for years under the *Gramm-Leach-Bliley Act* (GLBA). Far too often these companies are the targets of data thieves because they do not have the same standards in place as financial institutions. Credit unions suffer steep losses in re-establishing member safety after a data breach and are often forced to absorb fraud-related losses in its wake. Credit unions and their members are the victims in such a breach, as members turn to their credit union for answers and support when such breaches occur. As credit unions are not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs.

NAFCU believes that negligent entities should be held financially liable for any losses that occurred due to breaches on their end so that consumers are not left holding the bag. When a breach occurs, depository institutions should be made aware of the breach as soon as practicable so they can proactively monitor affected accounts. Finally, any new rules or regulations to implement these recommendations should recognize credit unions' compliance with GLBA and not place any new burdens on them.

As we have shared with you before, we recognize that a legislative solution to data security is a complex issue, and thus have established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other depository institutions are required to meet certain criteria for safekeeping consumers' personal information and are held accountable if those criteria are not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers other entities who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on depository institutions under the GLBA.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the negligent entity who incurred the breach.

NAFCU's Principles for a Federal Data Privacy Standard

Entwined 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 Subcommittee works to achieve a path forward on federal data privacy legislation, NAFCU recommends you include the following elements as key aspects in any such bill:

- **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 NCUA should be the sole regulator. Allowing 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 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 is 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.

Regulation of Fintechs and Nonbanks

As NAFCU testified before the Subcommittee in April 2021, the growth of fintech in recent years offers new opportunities for the delivery of financial services.[1] The use of financial technology can have a positive effect on credit union members. Credit unions have worked with fintech companies to improve efficiency in traditional banking, and many of the technologies that are commonplace today, such as credit cards and e-sign, would have once qualified as "fintech" when they were first introduced. Consumers today come to expect technological developments from their financial institution—from online banking to mobile bill pay. Many credit unions embrace innovations in technology to improve relationships with members and offer more convenient and faster access to financial products and services.

However, the growth of fintech can also present new threats and challenges as novel entities emerge in an underregulated environment. As such, NAFCU believes that Congress and regulators must ensure that when technology firms and fintechs compete with regulated financial institutions, they do so on a level playing field where smart regulations and consumer protections apply to all participants. NAFCU has outlined some of the challenges and opportunities in this area in a white paper which proposes regulatory recommendations for oversight of fintech companies.[2]

For example, 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 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.

[1] House Committee on Financial Services Subcommittee on Consumer Protection and Financial Institutions, "Banking Innovation or Regulatory Evasion? Exploring Trends in Financial Institution Charters," April 15, 2021, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=407533.
[2] NAFCU, Regulatory Approaches to Financial Technology, available at https://www.nafcu.org/fintech-whitepaper.

Congress should ensure that the data security and privacy requirements for financial institutions in the GLBA, including supervision for compliance, apply to all who are handling consumer financial information and that programs for implementing these requirements conform to the guidance developed by FFIEC member agencies.

NAFCU also believes financial regulators have a role to play in the supervision and regulation of fintechs under their existing authorities. Congress should also be willing to step in and clarify the role of regulators when necessary. For example, NAFCU believes that the Consumer Financial Protection Bureau (CFPB) can play a role under its "larger participants" authority under the Dodd-Frank Act to regulate and supervise technology firms and fintech companies that enter into the financial services marketplace. If the CFPB does not believe it has this authority currently, Congress should examine granting the Bureau explicit authority in this area.

Congress should also consider creating an FFIEC subcommittee on emerging technology to monitor the risks posed by fintech companies and develop a joint approach for facilitating innovation. We would envision the subcommittee having the following under its charge:

a. To report its findings to Congress annually;
b. To define the parameters of responsible innovation to ensure consistent examination of emerging technologies;
c. To identify best practices for responsible innovation; and,
d. To recommend regulatory improvements to allow FFIEC-regulated institutions to adopt new technologies with greater legal certainty.

Regulation of the Consumer Reporting Agencies (CRAs)

High-profile data breaches in recent years have highlighted the need for addressing consumer data security issues at national credit bureaus and beyond. While credit bureaus, such as Equifax, are governed by data security standards set forth by the GLBA, they are not examined by a regulator for compliance with these standards in the same manner as depository institutions. For example, the 2017 Equifax breach reportedly occurred via a "known" security vulnerability that software companies had issued a patch to fix several weeks prior. If Equifax had acted to remedy the vulnerability in a reasonable period of time, this breach may not have occurred. Companies that knew or should have known about a threat and failed to take mitigating action must be held financially liable.

When a breach occurs at a credit bureau, depository institutions should be made aware of the breach as soon as practicable so they can proactively monitor affected accounts and limit the losses that in credit unions are ultimately borne by the members. Furthermore, compliance by credit bureaus with GLBA and these notification requirements should be examined for, and enforced by, a federal regulator. We do believe that there should be further examination as to whether the CFPB – as proposed by the *Enhancing Cybersecurity of Nationwide Consumer Reporting Agencies Act* before the Subcommittee – or the Federal Trade Commission (FTC) is the best approach to establishing appropriate standards in this area.

In conclusion, we appreciate the opportunity to share our input on this important topic and look forward to continuing to work with the Subcommittee on these issues. Should you have any questions or require any additional information, please contact me or Sarah Jacobs, NAFCU's Associate Director of Legislative Affairs, at sjacobs@nafcu.org.

Sincerely,

Brad Thaler

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Consumer Protection and Financial Institutions