



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

The Honorable Blaine Luetkemeyer
Chairman
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Wm. Lacy Clay
Ranking Member
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
U.S. House of Representatives
Washington, D.C. 20515

March 7, 2018

Re: Hearing on "Legislative Proposals to Reform the Current Data Security and Breach Notification Regime"

Dear Chairman Luetkemeyer and Ranking Member Clay:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write today in conjunction with today's hearing on data security to share our thoughts on the broader topic and the specific bills before you today. We appreciate the Subcommittee's continued focus on this important topic and need for addressing consumer data security issues. As NAFCU testified before the Subcommittee last November, there is a 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. We are pleased to see the Subcommittee is continuing its work on this important topic.

NAFCU's Principles on Data Security

As our testimony noted, we recognize that a legislative solution 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 *Gramm-Leach-Bliley*

Act (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.

The Data Acquisition and Technology Accountability and Security Act

NAFCU is pleased to see the draft legislation proposed by Chairman Luetkemeyer and Representative Maloney which would establish a national standard for both data security and breach notification, while recognizing the existing framework from the GLBA that has been in place for financial institutions for nearly two decades. We also appreciate that the legislation maintains the status quo on the ability of credit unions to take a private right of action to recoup costs suffered in a data breach.

As the Subcommittee examines the discussion draft, we would encourage you to clarify and

make improvements to the draft. For example, in Section 4 dealing with notification, the timeline for notice to consumers is “immediately notify without unreasonable delay,” which could lead to confusion and may interfere with law enforcement efforts. We believe timely notification is critical, but would urge greater clarity of this provision. We would also like to see greater clarity on the requirements to provide timely notification to financial institutions holding accounts of consumers who have been victims of a data breach.

We also believe that there should be some technical fixes and clarity in Section 5 to ensure that credit unions that are bound by GLBA are deemed in compliance with the data security requirement in Section 3 and the breach notice requirement in Section 4. We believe that this is the intent of this section, but believe it is unclear if the proposed language would accomplish that.

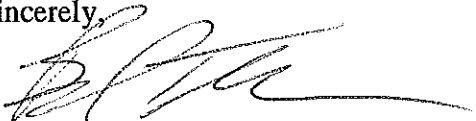
NAFCU is supportive of the efforts with this legislation and we stand ready to work with you on this bill as it moves forward in the legislative process.

H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act of 2017

NAFCU is supportive of Title I of H.R. 4028, the *PROTECT Act of 2017*, offered by Representative McHenry, which would subject large consumer reporting agencies to supervision and examination by the Federal Financial Institutions Examination Council (FFIEC). This would help address some of the concerns about the gaps in regulation of large credit rating agencies. While we believe there could be merit behind the proposals in Title II to establish a system for a national security freeze and Title III’s phase-out of the credit rating agency use of Social Security Numbers, we believe these topics need further study for potential broader impacts and to avoid unintended negative results.

On behalf of our nation’s credit unions and their more than 110 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 Allyson Browning, NAFCU’s Associate Director of Legislative Affairs, at 703-842-2836 or abrowning@nafcuh.org.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

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