



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

October 16, 2020

The Honorable Mitch McConnell
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Charles E. Schumer
Minority Leader
United States Senate
Washington, D.C. 20510

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

Re: Recent Breaches Highlight Continuing Need for Congress to Address Data Security

Dear Leader McConnell, Speaker Pelosi, Leader Schumer and Leader McCarthy:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) to urge you to keep data security concerns on the Congressional agenda. As you are aware, NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve 122 million consumers with personal and small business financial service products.

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. In light of the pandemic, digital and card transactions are on the rise, potentially putting more consumer information at risk. Just this week, new breaches have been announced at Barnes & Noble bookstores, Dickey's Barbecue and Robinhood Markets. While exact details of these breaches are still emerging, the Robinhood breach at least appears to have compromised funds in some customer accounts. These breaches are just another reminder that it is time for Congress to act to prevent future breaches and harm to consumers. We would urge your continued focus on this important topic and the need for addressing consumer data security issues in the remaining days of this Congress and in the new Congress.

Unfortunately, retailers, and even fintechs such as Robinhood, 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). Even more troubling, the U.S. Securities and Exchange Commission (SEC) issued an advisory last month which warned against precisely the sort of authentication weaknesses that may have played a role in the reported Robinhood breach.¹ Given that Robinhood has suffered high profile breaches in the past, it may be that the SEC's regulatory toolkit needs updating. In this context, it may be appropriate for Congress to ask why the agency has so far declined to extend the scope of its Systems Compliance and Integrity

¹ SEC, Risk Alert: Cybersecurity: Safeguarding Client Accounts against Credential Compromise (September 15, 2020), available at <https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf>.

regulation (Reg SCI) to retail broker-dealers like Robinhood that handle the transactions of millions of users.² As past data security incidents have often shown: in hindsight, breaches can be prevented. NAFCU believes that when a breached entity knew or should have known about a threat, and fails to act to mitigate it, the negligent company must be held financially liable.

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 victims in this 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.

NAFCU's Principles on Data Security

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.

² See SEC, Regulation Systems Compliance and Integrity, 79 Fed. Reg. 72251 (December 5, 2014). Regulation SCI requires SCI entities to take corrective action with respect to SCI events, defined to include systems disruptions, systems compliance issues, and—most notably—systems intrusions, and notify the SEC of such events. But SCI entities do not appear to cover order-entry firms or clearing broker-dealers.

- **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.

We urge you to keep data security high on the Congressional agenda, both in the waning days of this Congress and when the 117th Congress convenes in January.

On behalf of our nation's credit unions and their 122 million members, we thank you for your attention to this important matter and stand ready to work with you. Should you have any questions or require any additional information, please contact me or Sarah Jacobs, NAFCU's Associate Director of Legislative Affairs, at 703-842-2231 or sjacobs@nafcu.org.

Sincerely,



Brad Thaler
Vice President of Legislative Affairs

cc: Members of the U.S. Senate
Members of the U.S. House of Representatives