June 16, 2014

The Honorable Harry Reid
522 Hart Senate Office Building
Washington, DC 20510

The Honorable Mitch McConnell
317 Russell Senate Office Building
Washington, DC 20510

The Honorable John Boehner
1011 Longworth House Office Building
Washington, DC 20515

The Honorable Nancy Pelosi
235 Cannon House Office Building
Washington, DC 20515

Dear Leader Reid, Leader McConnell, Speaker Boehner and Leader Pelosi:

The National Association of Federal Credit Unions (NAFCU) recently sent a letter to Congressional offices on the issue of data security. NAFCU, an organization whose members suffer data breaches, should know better than to engage in the type of finger-pointing they put in their letter. First and foremost, we should recognize that businesses whose data is breached are victims of crime. While we can and should do more to try to prevent such crimes, we ought to keep that in mind.

We should also recognize that, according to the Verizon data breach report, financial institutions are the victims of nearly 150% of the breaches that retailers are. NACFCU's letter failed to point that out. Retailers also suffer more of the losses from payment card fraud than do financial institutions and retailers spend more than $6.5 billion protecting against payment card fraud each year. And, in response to statements made earlier in the year by the Credit Union National Association (CUNA), we provided every congressional office with links to Visa and MasterCard rules as well as Federal Reserve regulations that establish that retailers prepay financial institutions for the costs of re-issuing cards due to fraud concerns and pay for the costs of fraud and re-issuing cards when retailers suffer data breaches. Financial institutions do not reimburse retailers for fraud costs retailers incurred when the financial institutions suffer data breaches. Nor, of course, do financial institutions object to getting paid for these costs twice.

Unfortunately, the debit and credit card products issued by financial institutions are fraud-prone. The reason why financial institutions and retailers are targeted for breaches so often is that criminals can make money if they simply get access to the account number that is embossed right on the front of these cards. In many other countries, the financial industry has taken steps to make account numbers by themselves far less useful to criminals. PIN numbers, for example, are required in some other countries. That means a criminal with an account number is prevented from buying anything with that account number alone. This isn't fool-proof, but it has been shown to cut fraud by about 84%. It is worth noting that credit unions and banks require the use of PIN numbers when their own funds are being accessed through ATM machines even though they don't allow the same precautions in many transactions with retailers.

The financial industry resistance to the use of PIN numbers – and, in fact, the practice of many credit unions of discouraging the use of PIN by charging their customers for using PIN numbers – directly contradicts our shared interest in improving data security. And, of course, it demonstrates in a concrete way that financial institutions are more focused on the higher fees they make from non-PIN transactions than they are in protecting consumers.

It may be helpful to examine some of the points that NAFCU recommends in its letter as priorities for legislation before deciding how to approach these issues.

- NAFCU asks for breached entities to pay breach costs: As noted, retailers already pay the costs of fraud and the costs of re-issuing cards twice through swipe fees and reimbursement payments. Banks and credit unions do not pay for retailers' breach costs when the banks/credit unions are breached so adding the same responsibility onto banks/credit unions may be a point of common ground – especially if NAFCU thinks breached entities should only pay once as that would entitle retailers to substantial refunds.

- NAFCU asks for national standards for safekeeping information: National standards should cover everyone involved in keeping key financial information of consumers. Unfortunately, the Gramm-Leach-Bliley Act does not create the type of standard that NAFCU advocates. GLBA has financial institutions make their own evaluations and tailor policies and procedures to what they believe to be appropriate. Then, they report what they've done to their boards. There is no substantive oversight of these standards even though examiners look to ensure the policies are in place. This may be why many credit unions and banks are not able to accept encrypted data when processing transactions. Because they can't accept encrypted data, retailers or their processors have to de-encrypt financial data before sending it, and that creates risk for breaches.

- NAFCU asks for disclosure of the breached entity, but GLBA does not require financial institutions to disclose that fact when they are breached. In fact, we have found that financial institutions have at times blamed retailers when those retailers were not the source of the breach.

- NAFCU's request to limit data retention is remarkable because the primary reason many retailers need to retain card account information is that the credit card companies can challenge those charges and take retailers' funds several months after a transaction occurs. Retailers must retain transaction information to protect against this. If the credit card companies stopped taking retailers' funds in those situations, far less data would need to be retained.

Overall, NAFCU's letter is more significant for what it doesn't say than for what it does say. It is unfortunate that NAFCU would rather try to assign blame than constructively find ways to address the problems of data breach and fraud. Several merchant and financial industry groups have been working together constructively for months to try to do that. NAFCU ought to re-evaluate whether it is helping or hurting the effort to improve data security.

Sincerely yours,

Lyle Beckwith
Senior Vice President, Government Relations

Cc: Members of the US Senate and House of Representatives