



October 6, 2014

The Honorable Barack Obama
President of the United States
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

We feel compelled to respond to the letter that the National Association of Federal Credit Unions (NAFCU) sent on September 26th 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 Investigations Report, the most comprehensive summary of these types of threats, there were 1,367 data security incidents with confirmed data losses in 2013. Of those, the financial industry suffered 34%, public institutions (including governmental entities) had 12.8%, the retail industry had 10.8%, and hotels and restaurants combined had 10%. Given these figures, and the news that 76 million accounts were compromised in the recent JP Morgan Chase breach, the financial industry should not be pretending that data security is a retail problem.

We would also note that merchants suffer more of the losses from payment card fraud than do financial institutions and merchants spend more than \$6.5 billion protecting against payment card fraud each year. Visa and MasterCard rules and Federal Reserve regulations demonstrate that merchants prepay financial institutions for the costs of re-issuing cards due to fraud concerns, prepay the fraud losses that financial institutions may have on payment cards and then pay again for the costs of fraud and re-issuing cards when merchants suffer data breaches. Financial institutions do not reimburse merchants for fraud costs merchants incur 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 merchants 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 merchants.

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, merchants 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 merchants' 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 merchants 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, merchants 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 merchants when those merchants were not the source of the breach.
- NAFCU's request to limit data retention is remarkable because the primary reason many merchants need to retain card account information is that the credit card companies can challenge those charges and take merchants' funds several months after a transaction occurs. Merchants must retain transaction information to protect against this. If the credit card companies stopped taking merchants' 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. In our view, progress can only be made on these important issues if we look objectively at facts rather than distracting from the real issues by looking for a scapegoat. We look forward to working with you to find real solutions.

National Association of Convenience Stores
National Grocers Association
National Restaurant Association