October 30, 2014

Mr. Jim Nussle
President and CEO
Credit Union National Association
601 Pennsylvania Ave NW, South Bldg.
Washington DC 20004

Mr. Dan Berger
President and CEO
National Association of Federal Credit Unions
3138 10th Street North
Arlington, VA 22201

Dear Mr. Nussle and Mr. Berger,

We are writing to address a number of misleading and factually inaccurate points perpetuated by the Credit Union National Association (CUNA), the National Association of Federal Credit Unions (NAFCU) and other state credit union associations in the media and before Congress in regards to the state of cybersecurity in our country. As parts of the same payment ecosystem, it is important that our shared goals remain the improvement of cybersecurity and protection of consumers.

To begin with, we would like to take this opportunity to dispel a few misconceptions which seem to have arisen regarding recent cyber-attacks and the response by retailers and financial institutions. These misconceptions are as follows:

- **Data breaches only – or disproportionately – affect retail merchants.**

  We know that this can be easily disproved by both empirical evidence and recent high-profile occurrences. When the 2014 Verizon Data Breach Investigations Report analyzed 1,367 data-loss incidents last year, they found that 465 (roughly 34 percent) took place at financial institutions, while fewer than 150 (less than 11 percent) affected retailers. Furthermore, the recent breach at J.P. Morgan Chase & Co. – one of the largest financial institutions in the world – is reported to have compromised the information of some 76 million households and 7 million businesses. And, as the USA Today reported on its front page October 20th, "Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building." It is important to realize that both retailers and financial institution have been affected by cyber-attacks and both likely will be again.

- **Retailers do not share the costs incurred by card fraud.**

  A 2013 study by the Federal Reserve looked at fraud instances associated with use of debit cards and found that retailers do share the costs incurred as a result of card fraud. In fact, costs were shown to be borne almost equally among retailers and card-issuing institutions.

These vary by transaction: for more secure PIN debit transactions the card issuer, naturally, absorbed a greater share of the fraud; for less secure signature debit transactions the merchants absorbed nearly half of all fraud losses; and for card-not-present debit transactions (transactions made online, over the telephone or by catalogue) merchants bore a greater percentage of fraud losses than card issuers did. And, merchants pay the cost of card fraud in advance, through swipe fees, before fraud is ever incurred. In fact, even the Federal Reserve's debit card regulations are geared to provide that the average issuer has one hundred percent of its debit fraud losses covered by swipe fees. Moreover, even after absorbing substantial fraud losses, merchants are subject to massive fines by Visa and MasterCard networks and hundreds of millions of dollars in restitution through private litigation for cybersecurity breaches.

- **Retailers do not contribute to the costs of issuing new cards to consumers after a data breach.**

Merchants do, in fact, reimburse card issuers for both card reissuance and actual fraud losses following a breach based on many factors, including: the number of cards requiring reissuance, the incremental fraud associated with each individual card, and the age of the card and when it was due for reissuance, regardless of a breach. These schedules are contractually agreed upon by Visa and MasterCard and your credit union members. Merchants do not have a say in these reimbursement requirements. For example, MasterCard reimburses card issuers on the following schedule for card reissuance:

Reimbursement Rate Per Tier

Tier	Issuer—Gross Dollar Volume	Mag Stripe	Chip[2]	*PayPass*	Combo[3]
1	0–200 MM	USD 2.69	USD 3.66	USD 3.44	USD 4.04
2	201 MM–1 B	USD 2.31	USD 3.29	USD 3.06	USD 3.66
3	> 1B	USD 2.00	USD 2.98	USD 2.75	USD 3.35

A fixed deductible of 40 percent is subtracted from the gross eligible reimbursement amount to reflect anticipated card expirations and accounts published in previous MasterCard Alerts.

This chart clearly demonstrates that a credit union with assets of under $200 million is eligible to receive a higher reimbursement rate than its larger competitors. Additionally, if there is fraud associated with the card, card issuers are again eligible for a separate fraud adjustment reimbursement.

To support our insistence that CUNA and NAFCU stop repeating such false statements as "merchants bear NONE of the costs to issue…new credit and debit cards," "merchants pay nothing when they lose my personal data, [and so] they have no reason to make their data

protection standards more stringent," and "when the merchants cause a data breach, they just pass along all the costs…to my credit union," we bring to your attention the specific sections of MasterCard's operating rules where these sections may be found: 6.4.1 ADC Operational Reimbursement Factors, MasterCard Account Data Compromise User Guide, July 22, 2012. Of course, Visa maintains similar schedules to which your credit unions have contractually agreed to as well.

- **Retail merchants leave the burden of customer security exclusively up to credit unions and banks.**

  Just as data breaches are a shared threat, protecting against them is a shared responsibility. Merchants spend more than $6 billion annually on data security. And retailers already employ a number of methods to protect against card fraud, including:

  - PIN prompting at the point-of-sale for debit cards
  - Card Verification Value (CVV) prompting for Internet purchases
  - Address/ZIP code verification
  - Automated transaction scoring
  - Data encryption
  - Data tokenization
  - Internet Protocol (IP) address/geolocation authentication

Merchants pay financial institutions extra fees for some of these services. And, in addition to the safeguards listed above, retailers are proactively leading the way in advancing technology that would significantly increase protection for consumers: Chip-and-PIN payment cards.

The volume of cyber-attacks has become particularly intense because the antiquated and woefully inadequate magnetic stripe technology still in place today. As issuing banks in nearly every other G-20 nation have migrated away from this 1960s-era technology to a substantially more secure technology, known as Chip-and-PIN, cybercrime and fraud have migrated to the United States. Retailers are on track to have completed an enormous investment in order to be able to accept Chip cards next year. Yet, there is still little promise that card issuers will issue such cards. In fact, financial institutions trail merchants on these technology updates in the United States and around the globe. Outside of the U.S., 70 percent of merchants have upgraded to Chip-and-PIN devices at the point-of-sale, but only 40 percent of the cards have been upgraded. That is similar to the situation here in the United States where nearly 20 percent of merchants have upgraded their terminals but less than one percent of the cards issued contain the new technology.

Moreover, card issuers in the United States intend to begin issuing chip cards without requiring PINs, a feature that is proven to reduce fraud by 700 percent on debit cards alone. If this occurs, it will result in an inexcusable lapse which threatens to make billions of dollars in merchant upgrades ineffective. It is difficult to ignore the benefits of PINs for enhanced security when credit unions themselves require them for withdrawals at their own ATMs.

Reportedly, credit unions will not be issuing chip cards by the timelines set by the financial industry. According to the *Credit Union Times*, more than half of all credit unions are expected to miss an October 2015 date to issue cards equipped with chips. In discussing the migration to payment cards with chips, Barney Moore, manager of card consulting services for Card Services for Credit Unions (CSCU), an association of credit unions affiliated with payment processor FIS, recently told the *Credit Union Times*, "it seems unlikely that they [credit unions] will have gotten it done by next October." Moore cited concerns about "costs, delays in ironing out technical details and bottlenecks among plastic card suppliers" as reasons credit unions could miss the mark. If merchants will collectively be spending $30 billion to upgrade their terminals by October 2015, it is unfathomable that credit unions are not willing to upgrade magnetic stripe cards, which cost $1 to issue, to more secure chip cards, which only cost an additional $3 to issue.

Protecting our customers is a shared interest and we must all work to ensure the highest level of security possible. Instead of engaging in finger-pointing, all participants in the payments ecosystem must put in place measures that are effective, be vigilant, and embrace collaborative public-private partnerships that are available and proven to work. The bottom line is that consumers and accountholders deserve solutions, not posturing and misinformation. For these reasons, the merchant community is working together with many within the financial services industry to strengthen protections for consumers. The Merchant-Financial Services Cyber Security Partnership is a collaborative effort that has brought together more than 250 executives from all segments of the merchant and financial services communities to work with their peers to protect their shared customers.

Unfortunately, while retailers, restaurants, convenience stores, hotels, national banks, card networks and community banks have joined the Partnership, one constituency has still not seen fit to participate: credit unions. It is past time we started working together for the greater good of America's consumers.

Sincerely,

Sandra L. Kennedy
President
Retail Industry Leaders Association

Henry Armour
President and CEO
National Association of Convenience Stores

Matthew R. Shay
President and CEO
National Retail Federation

Peter J. Larkin
President and CEO
National Grocers Association

Leslie G. Sarasin, Esq., CAE
President and CEO
Food Marketing Institute

Mark Horwedel
CEO
Merchant Advisory Group