November 3, 2014

Sandra Kennedy
President
Retail Industry Leaders Association

Peter J. Larkin
President and CEO
National Grocers Association

Henry Armour
President and CEO
National Association of Convenience Stores

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

Matthew R. Shay
President and CEO
National Retail Federation

Mark Horwedel
CEO
Merchant Advisory Group

Dear Ms. Kennedy, Mr. Armour, Mr. Shay, Mr. Larkin, Ms. Sarasin and Mr. Horwedel:

Thank you for your October 30, 2014, letter regarding the state of cybersecurity in our country. As not-for-profit cooperatives, credit unions serve over 100 million members and meet the financial service needs of consumers and small businesses throughout the country. Please be assured that our associations have a vested interest in this issue and share in the goals of improving cybersecurity and better protecting American consumers.

Addressing ongoing data security breaches is imperative for credit unions and their members, and we are eager to help find solutions that will minimize such breaches and the costs credit unions must incur in their wake. You have asked us to join in a Merchant-Financial Services Cyber Security Partnership. We appreciate that when differing parties come together, it is possible that positive discussions can occur and agreements can be reached. To that end, we gave considerable consideration to the question of whether to join this group several months ago and concluded that discussions simply would not be productive as long as merchants are not willing to do their part to safeguard consumers' financial data.

Merchants and financial institutions both play critical roles in the payments system and they should be held to similar standards with respect to protecting consumer data. The weak link in the system today is on the merchant end. We continue to work with our members to deploy new technology, but as long as the security standards on the merchant side of the system are weaker than those on the financial institution side of the system, the vulnerability for consumers and financial institutions will be at your feet.

Credit unions and other financial institutions already have procedures in place designed to prevent data breaches and to minimize the impact on consumers should a breach occur. Furthermore, the credit unions themselves are financially responsible for losses that their members may suffer as a result of a merchant's data breach.

We agree that improved technology can help reduce fraud and strengthen data security, but in order for consumers to be more reasonably protected, advances in technology must be accompanied by merchants' compliance with federal standards for the safe keeping of financial data, cost liabilities, and breach notifications in the event of an attack. This is reasonable and the right thing to do. Further, we believe it would be good business for merchants to do all they can to protect consumers' financial data.

To date, the Target and Home Depot breaches alone have cost credit unions and their member-owners at least $90 million. This exorbitant cost not only hurts credit unions but also the consumers that they serve. There is no end in sight as long as you resist federal data security standards, like those credit unions must follow under the Gramm-Leach-Bliley Act.

In sum, despite our past differences on other significant issues, we are willing to join a collaborative effort to improve the security of the payments system but only if your members are willing to accept their responsibilities to meet data security-related standards that credit unions and other financial institutions are held to today.

Sincerely,

B. Dan Berger
NAFCU
President & CEO

Jim Nussle
CUNA
President & CEO