February 3, 2014

The Honorable Mark Warner
Chairman, Subcommittee on National Security and International Trade and Finance
U.S. Senate
Washington, D.C. 20510

The Honorable Mark Kirk
Ranking Member, Subcommittee on National Security and International Trade and Finance
U.S. Senate
Washington, D.C. 20510

Re: Hearing Titled "Safeguarding Consumers' Financial Data"

Dear Chairman Warner and Senator Kirk:

The undersigned organizations representing the financial services industry are writing to commend you for holding this hearing on the recent breaches of sensitive consumer financial and personal information at several major retailers across the country. The financial services industry stands ready to assist policymakers in ensuring that robust security requirements apply to all participants in the payments system, and we respectfully request that this letter be made part of the record for your hearing.

In all data breaches, including the recent retailer breaches, the financial services industry's first priority is to protect consumers from fraud caused by the breach. Banks and credit unions do this by providing consumers "zero liability" from fraudulent transactions in the event of a breach. Although financial institutions bear no responsibility for the loss of the data from a retailer's system, they assume the liability for a majority of the resulting card-present fraud. In most instances, financial institutions have historically received very little reimbursement from the breached entities – literally pennies on the dollar.

For example, virtually every bank and credit union in the country is impacted by the Target breach. Our understanding is that the breach affects up to 40 million credit and debit card accounts nationwide, and also has exposed the personally identifiable information (name, address, email, telephone number) of potentially 70 million people. To put the scope of the breach in perspective, on average the breach has affected 10 percent of the credit and debit card customers of every bank and credit union in the country.

The Target breach alone is estimated to cost financial institutions millions of dollars to reissue cards and increase customer outreach, with substantial longer-term costs associated with fraud and mitigation efforts to limit the damage to customers. Although a variety of factors can go into the calculation, for banks and credit unions the cost of reissuing cards can range from $5 up to $15 per card, and a preliminary survey of banks impacted by the Target breach conducted by the Consumer Bankers Association indicated that more than 15.3 million debit and credit cards have been replaced to date. The numbers of cards issued, along with the total costs, are nearly certain to rise, especially as the extent to which other retailers have been breached becomes more certain.

For consumers, the critical issue is the security of their personal information. Banks, credit unions, and other financial companies dedicate hundreds of millions of dollars annually to data security and adhere to strict regulatory and network requirements at both the federal and state levels for compliance with security standards. However, criminal elements are growing increasingly sophisticated in their efforts to breach vulnerable links in the payments system where our retailer partners have not yet been able to align with the financial sector's higher standards of practice in security. In fact, according to the Identity Theft Resource Center, there were more than 600 reported data breaches in 2013 – a 30 percent increase over 2012. The two sectors reporting the highest number of breaches were healthcare (43 percent) and business, including merchants (34 percent). Because of the Target breach, the business sector accounted for almost 82 percent of the breached records in 2013. In contrast, the financial sector accounted for only 4 percent of all breaches and less than 2 percent of all breached records.

Our payments system is made up of a wide variety of players: financial institutions, card networks, retailers, processors, and new entrants. Protecting this eco-system is a shared responsibility of all parties involved and all must invest the necessary resources to combat increasingly sophisticated breach threats to the payments system.

Indeed, extensive efforts are under way to improve card security, including implementation of EMV (chip-based technology) standards by encouraging investment in point-of-sale terminal upgrades and card reissuance to accommodate EMV transactions, and investing in additional security innovations. The major card networks started the EMV migration domestically in 2011, and in 2015 at the retail point-of-sale the party that is not EMV capable (either the issuer or merchant) will be responsible for counterfeit fraud. EMV migration will be fully implemented by October 2017. This liability shift incentivizes both retailers and financial institutions to implement chip-based technology.

EMV technology improves current security by generating a one-time code for each transaction, so that if the card number is stolen it cannot be used at an EMV card-present environment. This is core to our concern with requiring PIN as a cardholder verification method. Imagine if more PINs were used at the check-out, and they were stolen at the same magnitude as account numbers. The level of resulting ATM fraud would be staggering. Also, while EMV addresses card-present fraud, it does not increase the security of on-line transactions, which is an increased target in countries that have implemented EMV.

Threats to data security are ever changing and unpredictable. Therefore, policymakers should not mandate or embrace any one solution or technology, such as EMV, as the answer to all concerns. As the threat evolves, so too must coordinated efforts to combat fraud and data theft that harm consumers. To address the emerging risks posed by mobile payments, for example, industry-driven solutions, such as the TCH Secure Cloud, are already underway employing "tokenization" technology.

Tokenization adds additional security by generating a random limited-use number for e-commerce or mobile transactions, rather than using the actual account number. If stolen and attempted to be used as a legitimate account number, it would be of limited to no use. It also takes merchants out of harm's way by eliminating the need for them to even store sensitive

account numbers. As threats continue to evolve, so to must our efforts to combat fraud and data theft that harm consumers, financial institutions, and the economy.

As you and your colleagues consider next steps for dealing with this important issue, we have several recommendations that would help to strengthen the payments system and better protect consumers in the event of a breach.

1) **Establish a national data security breach and notification standard.** We believe that legislation should be enacted to better protect consumers by replacing the current patchwork of state laws with a national standard for data protection and notice. A good example of this is the Data Security Act of 2014 (S. 1927) introduced by Senators Tom Carper (D-DE) and Roy Blunt (R-MO).

2) **Make those responsible for data breaches responsible for their costs.** Financial institutions bear the brunt of fraud costs. An entity that is responsible for a breach that compromises sensitive customer information should be responsible for the costs associated with that breach to the extent the entity has not met necessary security requirements.

3) **Better Sharing of Threat Information**. Unnecessary legal and other barriers to effective threat information sharing between law enforcement and the financial and retail sectors should be removed through private sector efforts and enactment of legislation. For example, one such private sector effort is the expansion of membership in the Financial Services Information Sharing and Analysis Center to include the merchant community. No one organization or sector alone can meet the challenges of sophisticated cyber-crime syndicates, so robust communities of trust and collective protection must constantly be developed.

Our organizations and the thousands of banks, credit unions, and financial services companies we represent are aggressively investing in a safe and secure payments system for our nation. Protecting this system is a shared responsibility of all parties involved and we need to work together to combat the ever-present threat of criminal activity. The financial services industry stands ready to assist policymakers in ensuring that robust security requirements apply to all facets of the payments system.

Sincerely,

American Bankers Association
The Clearing House
Consumer Bankers Association
Credit Union National Association
Financial Services Information Sharing and Analysis Center
The Financial Services Roundtable
Independent Community Bankers of America
National Association of Federal Credit Unions

Cc: Members of the Senate Banking Committee