American Bankers Association
Building Success. Together.

Frank Keating
President & CEO
202-663-5111
fkeating@aba.com

January 16, 2014

To: Members of the U.S. Senate
Members of the U.S. House of Representatives

From: Frank Keating, President and CEO, American Bankers Association

Subject: Target Data Breach

The recent data security breach at one of America's largest retailers, Target Corporation, has reignited the long-running debate over consumer data security policy. ABA and the thousands of community, mid-size, regional, and large banks we represent recognize the paramount importance of a safe and secure payments system to our nation and its citizens and welcome this ongoing discussion.

While the facts of this massive breach remain fluid, Target has acknowledged that the breach occurred within its internal systems, affecting nearly 40 million credit and debit card accounts, and revealed the personally identifiable information (e.g., name, address, email, telephone number) of potentially 70 million people. From ABA's perspective, Congress should examine the specific circumstances of this breach and the broader data security issues involved, and we stand ready as a resource to assist in your efforts.

To the extent it is helpful in your deliberations, it may be useful to consider the following points:

- **Banks Protect Consumers:** In breaches like that of Target's, the banking industry's first priority is to protect consumers and make them whole. When a retailer like Target speaks of its customers having "zero liability" from fraudulent transactions, it is because ***our nation's banks*** are providing that relief, not the retailer that suffered the breach. It is often the case that banks must explain to their customers what has happened without the bank knowing where the breach has occurred. Moreover, bankers have historically received little meaningful reimbursement for the costs they have incurred.

- **A Diverse Payments System with Multiple Players:** The payments system is made up of a wide variety of players: banks, card networks, retailers, processors, and even new entrants, such as Square, Google, and Paypal. Banks dedicate hundreds of millions of dollars annually to data security, and adhere to strict regulatory and network requirements. Banks are also subject to robust oversight and examination at both the federal and state levels. The same may not be true for other players.

- **Extensive Efforts in Card Security are Ongoing:** Extensive efforts are already under way to improve card security, including the implementation of EMV standards (e.g., chip-and-pin technology, set in motion by the networks in 2011 and to be fully implemented by 2015), and tokenization (e.g., technology to substitute heavily encrypted pieces of data for key elements of a person's financial information involved in the course of a transaction). These changes require significant financial investment by all parties – and have been the subject of some criticism by many, including parts of the retail industry – but are moving forward.

- **The Criminal Threat Continues to Grow:** As evidenced by the Target breach, criminal elements are growing increasingly sophisticated in their efforts to breach the payments system, requiring ***all participants in the payments system*** to invest the necessary resources to combat what is a dynamic and continually changing threat. Inter-industry squabbles, like those over interchange, have had a substantial impact on bank resources available to combat fraud. Policymakers must examine that impact closely to ensure that the necessary resources are not diverted from addressing the real concern at hand – the security of our nation's payment system and the need to protect consumers.

- **Security Protections Must Continue to Evolve:** There is no panacea for the ever-changing threats that exist today, or that can anticipate what new challenges will come years from now. Policymakers should be cautious not to embrace any "one" solution that's being pushed by some as the answer to all concerns. For example, EMV technology helps to address potential fraud at the cash register (known as the "point-of-sale" or POS location); it does not address on-line security, nor is it a perfect solution even at the POS as criminal efforts evolve. In fact, security experts suggest that such EMV technology would not have fully prevented the potential harm of the Target breach.

Much has recently been made about the on-going disagreements between the retail community and the banking industry over who is responsible for protecting the payments system. In our view, it is a ***shared responsibility of all parties involved***. Our existing payments system serves hundreds of millions of consumers, retailers, banks, and the economy well, and we must work together to combat the ever-present threat of criminal activity at our collective doorstops.

Thank you for considering our views. ABA and the banking industry's two million employees stand ready to assist you as we jointly combat threats to our system.