January 28, 2014

U.S. House of Representatives
Washington, D.C. 20515

Dear Representative:

On behalf of the thousands of community financial institutions we represent, the Independent Community Bankers of America (ICBA) and the National Association of Federal Credit Unions (NAFCU) jointly call on Congress to advance reforms to effectively secure consumer financial data. In the wake of recent, wide-scale data breaches at Target, Neiman Marcus and other retailers, which have jeopardized more than 100 million individuals, the need for Congressional action has never been greater. Though our policy interests sometimes diverge, when it comes to the financial integrity of our customers and members our concerns are completely aligned. Strong legislation is needed to restore confidence in our payments system which is critical to sustaining consumer spending and the economic recovery. Any reforms should:

Apply Gramm-Leach-Bliley Act (GLBA)-like standards to all entities that store consumer financial data. Since its passage in 1999, GLBA has worked effectively in protecting consumer data at financial institutions – banks, thrifts, and credit unions. No comparable data security standards apply to retailers, data processors and brokers, or other entities that store consumer data. This gaping loophole, which has created significant risk and given rise to the recent breaches, must be closed. An important part of this standard is the requirement for timely notification when a data breach occurs.

Ensure that the party at fault for a breach is liable for all losses. When payment card information is compromised, mitigation costs are significant. These include the costs of reimbursing consumers for fraudulent transactions, notification of at-risk consumers, issuance of new cards, changing account numbers, monitoring for fraudulent activity, and the increased customer service demands that inevitably follow a major breach. The cost of reissuing a single payment card alone may be as high as $10 to $15 for smaller institutions. A bank or credit union may have to reissue thousands of cards in the event of a major breach. The party at fault for a breach should bear responsibility for these costs. This change would better align incentives to keep consumer data safe and foster good business practices.

Create a single national standard. Many states have enacted laws with differing requirements for protecting consumer information and giving notice in the event of a data breach. This patchwork of state laws only fosters confusion and ultimately is detrimental to consumers. A single federal standard would strengthen data protection by promoting compliance and consumer understanding.

These are just a few of the important provisions that should be included in any data security legislation.

Finally, while some argue for financial institutions to expedite a switch to a "chip and pin" technology, we must point out that the reality is that "chip and pin" is no panacea for data security. "Chip and pin" cards can be compromised and used in online purchase fraud, as the technology is designed to hinder card duplication and card information can still be compromised. While card technology is continuing to evolve, so are the criminals that pursue personal financial data. The best way to truly help protect consumer financial information is to enact comprehensive national data security standards that stand up no matter what the technology.

Confidence in the payments system is a critical component of the economic recovery. ICBA and NAFCU urge Congress to make financial data security a priority issue in 2014. We would welcome the opportunity for our associations to share our thoughts with you during Congressional hearings examining the adequacy of merchant data security and the need for strong and effective legislation to close retailer security gaps and restore consumer confidence.

Thank you for your consideration.

Sincerely,

B. Dan Berger
President and CEO
NAFCU

Camden R. Fine
President and CEO
ICBA