September 9, 2014

U.S. Senate
Washington, DC 20510

Dear Senator:

The recent retailer security breach at Home Depot, together with earlier breaches at Target, Neiman Marcus and other retailers has affected more than one hundred million American consumers and no doubt raised concerns among your constituents, whether or not they were directly affected. These compromises at mass retailers undoubtedly have the potential to shake consumer confidence.

Community banks are strong guardians of the security and confidentiality of sensitive customer information as a matter of good business practice and legal and regulatory requirements. Safeguarding customer information is central to maintaining public trust and the key to long-term customer retention.

With a critical stake in the security of consumer data, Congress needs to reassess our federal data security and fraud laws. This is why ICBA continues to advocate our key data security principles to Congress and the payment card networks. ICBA's core principles include:

- the costs of data breaches should ultimately be borne by the party at fault for the breach,
- all participants in the payments system—including merchants—should be subject to Gramm-Leach-Bliley Act–like data security standards,
- a national data-security breach and notification standard should be implemented to replace the current patchwork of state laws,
- unnecessary barriers to effective threat-information sharing between law enforcement and the financial and retail sectors should be removed, and

- while community banks and other financial institutions continue to move to chip technology for debit and credit cards, these technologies alone may not have prevented the recent retailer breaches and do not protect against fraud in "card-not-present" transactions, such as online purchases.

We also want to use this opportunity to inform you of the actions taken by community banks to protect consumers. Community banks are committed to maintaining cardholder trust in the payments system through the following actions:

- Reassuring customers that community banks have multiple layers of security protection of personal information;
- Monitoring customer accounts for fraudulent activity;
- Informing customers that they bear zero liability for fraudulent transactions; and
- Educating customers on how to avoid fraud.

Thank you for your consideration.

Sincerely,

/s/

Camden R. Fine
President & CEO

1615 L Street NW, Suite 900, Washington, DC 20036-5623 | 800-422-8439 | FAX: 202-659-1413 | Email: info@icba.org | Website: www.icba.org