ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

March 5, 2014

# Retailer Data Breach: The Community Bank Perspective

On behalf of the nearly 7,000 community banks represented by the Independent Community Bankers of America (ICBA), thank you for convening today's hearing titled: "Data Security: Examining Efforts to Protect Americans' Financial Information." Community bankers and their customers are deeply alarmed by recent, wide-scale data breaches at prominent, national retail chains. These breaches have the potential to jeopardize consumers' financial integrity and confidence in the payments system. This confidence is vital to sustaining consumer spending necessary for the economic recovery. It is critical we determine what happened, identify the weakest links in the payments processing chain, and implement targeted changes to enhance consumer financial data security. We appreciate the opportunity to offer the community bank perspective on this important issue.

*Making Customers Whole*

In the wake of the retailer breaches, community banks have reissued more than four million credit and debit cards to consumers at a total reissuance cost of more than $40 million.[1] Reissuance costs are higher for community banks than for larger institutions that take advantage of economies of scale. Community banks absorb these costs upfront, even though the breaches occurred with retailers, because their primary concern is to protect their customers. Ultimately, these costs should be borne by the party at fault for the breach. This change would strengthen incentives for data protection. Because community banks acted quickly, initial fraud costs were relatively low. Less than one percent of community bank customers reported fraud on their accounts as a result of the recent breaches. These consumers are protected by a policy of zero-liability coverage. Financial institutions are required to provide this protection in order to issue Visa and MasterCard debit and credit cards.

While our current focus is on making customers whole, it is appropriate to begin to consider changes in policy, business practices, and technology that will strengthen payment system security and curb the risk of future breaches. The Joint Cybersecurity Partnership, joining ICBA and other financial services and retailer trade organizations, holds the promise of strengthening much needed cooperation across the payments chain.

*More Comprehensive Data Security Standards Are Needed*

Since 1999, financial institutions have been subject to rigorous data protection standards under the Gramm-Leach-Bliley Act (GLBA). These standards have been effective in securing consumer data at financial institutions. To adequately protect consumers and the payments system, **all** participants in the payments system should be subject to GLBA-like standards. Under current law, merchants and other parties that process or store consumer financial data are not

[1] Numbers are based on a sampling of community banks.

subject to federal data security standards. Securing financial data at banks is of limited value if it remains exposed at the point-of-sale and other processing points

*Liability Should Be Used To Align Incentives*

To maximize data security, the party that experiences a breach should bear responsibility for all costs associated with the breach. This change would better align incentives to keep consumer data safe and foster good business practices. As described above, when payment card information is compromised, mitigation costs are significant. If the party that experiences the breach does not bear these costs, they have little incentive to improve their data security.

*National Data Security Breach and Notification Standard is Vital*

Most states have enacted laws with differing requirements for protecting customer information and giving notice in the event of a data breach. This patchwork of state laws only increases burdens and costs, fosters confusion, and ultimately is detrimental to customers. Customer notification is important so that customers can take steps to protect themselves from identity theft or fraud. However, notification requirements should allow financial institutions and others flexibility to determine when notice is useful and appropriate. An overly broad notification standard that requires notice even when no threat exists will blunt the impact of notices that signal actual risk. Federal banking agencies should set the standard for financial institutions, as they currently do.

*New Technologies Will Reduce Risk But There Is No Universal Remedy*

Community banks are already investing in technologies that will better secure transaction processing and thwart criminals. In particular, community banks are joining other financial institutions in the orderly migration to chip technology for debit and credit cards. Chip technology may not have prevented the recent retailer breaches but it would have reduced the market value of the card data as it would be far more difficult for criminals to make counterfeit cards. Using chip technology will not protect against fraud in “card-not-present” transactions, such as online purchases. Criminals will continue to try to find weakness regardless of the technology so it is crucial that the marketplace continues to have the flexibility to innovate.

Thank you again for convening this hearing. ICBA looks forward to working with this Committee to craft targeted solutions to enhance the security of consumer financial data.