

Protecting Consumer Information: Can Data Breaches Be Prevented?

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: "Protecting Consumer Information: Can Data Breaches Be Prevented?" 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

While all the facts of these breaches are not yet known, community banks are taking actionable steps to make credit and debit customers whole. Consumers are protected by a policy of zero-liability coverage with regard to any fraud losses. This coverage is primarily provided by community banks and other financial institutions. Financial institutions are required to provide this protection in order to issue Visa and MasterCard debit and credit cards.

With a vital stake in containing the damage caused by breaches and restoring consumer confidence, community banks absorb the upfront costs of reissuing cards, responding to customer concerns and inquiries, protecting against fraud and any other expenses. These costs may be significant depending on the scope of the breach. For smaller institutions, the cost of reissuing a single credit or debit card ranges from \$10 to \$15. In a wide-scale breach even a community bank may have to reissue thousands of payment cards. Community banks absorb these costs upfront because their primary concern is to accommodate their customers. However, we strongly believe that these costs should ultimately be borne by the party that experiences the breach. This is critical to aligning incentives to maximize data security by all parties that store consumer data.

While our current focus is on making customers whole, it is appropriate to begin to consider changes in policy, business practice, and technology that will strengthen payment system security and curb the risk of future breaches.

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

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.

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.