November 1, 2017

Data Security: The Community Bank Perspective

On behalf of the more than 5,700 community banks represented by ICBA, we thank Chairman Luetkemeyer, Ranking Member Clay, and members of the Financial Services Subcommittee on Financial Institutions and Consumer Credit for convening today's hearing on "Data Security: Vulnerabilities and Opportunities for Improvement." The recent breach at Equifax highlights the urgent need for regulatory reforms to strengthen our payments and financial systems and deter future breaches. ICBA is pleased to have this opportunity to offer this statement for the hearing record.

Community banks are committed to safeguarding customer data and personal information. The community bank business model is founded on customer trust and service. Data security is a business imperative in the digital marketplace. Community banks invest significant and increasing resources in security controls to protect their consumers' data and critical systems.

ICBA and community bankers were appalled to learn of the massive data breach at Equifax involving 145.5 million American consumers. This breach has the potential to shake consumer confidence in our payments and financial systems for years. We urge Congress to take aggressive action to deter future breaches and mitigate the harm to consumers and to the financial system when breaches occur.

Examination and Supervision of Credit Reporting Agencies

Like financial institutions, the credit rating agencies (CRAs) are subject to the data security standards of the Gramm-Leach-Bliley Act (GLBA). Unlike financial institutions, CRAs are not examined or supervised for their compliance with these standards. This is a critical vulnerability. Significant third-party vendors that serve financial institutions are already subject to examination and supervision for compliance with GLBA standards. By the same logic, CRAs should be examined and supervised.

Create Incentives to Strengthen Data Security

Changes should not be limited to the CRAs but should extend to all entities that store personally identifiable consumer and financial data. Bad actors will continue to look for weaknesses in every link in the chain and future breaches will occur. To strengthen any weak links, ICBA recommends creating a legal structure in which the entity that incurs a breach – be it a retailer, CRA, financial institution, or other entity – bears liability for the cost of the breach.

When a breach occurs at any point in the chain, banks take a variety of steps to protect the integrity of their customers' accounts, including monitoring for indications of suspicious activity, changing customer identity procedures, responding to customer inquiries, reimbursing customers for confirmed fraudulent transactions, modifying customer limits to limit fraud losses, and blocking and reissuing cards of affected account holders at an estimated expense of up to $15 per card. Banks willingly bear these costs up front because prompt action following a breach is essential to protecting the integrity of customer accounts. But these costs should ultimately be borne by the entity that incurs the breach. This is not only a matter of fairness; a liability shift is needed to properly align

incentives for entities that store consumer financial and personally identifiable data to strengthen their data security. When breaches have a material impact on entities bottom line, they will quickly become more effective at avoiding them.

Additional Reforms

In addition to the reforms noted above, we urge Congress to consider comprehensive solutions which would include the following legal and regulatory changes:

- All participants in the payments and financial system, including merchants and CRAs, and all entities with access to customer financial information, should be subject to Gramm-Leach-Bliley Act-like data security standards and examined for compliance with those standards.
- Barring a shift in liability to the breached entity (as recommended above), community banks should continue to be able to access various cost recovery options after a breach.
- ICBA supports a national data security breach and notification standard to replace the current patchwork of state laws.
- Community banks should be notified of a potential and/or actual breach as expeditiously as possible in order to mitigate losses.

Unintended Consequences Must Be Avoided

ICBA is eager to work with this committee on constructive proposals to strengthen data security. In evaluating proposals, we ask this committee to be mindful of unintended consequences that could result for consumers, community banks, and the payments and financial systems. These systems are highly complex, and the consequences of ill-considered policies are hard to predict.

Closing

Thank you again for convening today's hearing. Data breaches are among the highest concerns of America's community bankers. ICBA looks forward to continuing to work with the committee to promote customer security and protect against costly and damaging data breaches.