February 14, 2018

Data Security: The Community Bank Perspective

On behalf of the nearly 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 "Examining the Current Data Security and Breach Notification Regulatory Regime." ICBA is pleased to have the 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 also urges Congress to be part of the data security solution by taking aggressive action as described below.

Examination and Supervision of Credit Reporting Agencies

The Equifax breach shows the ongoing vulnerability of credit reporting agencies (CRAs). While CRAs are subject to the data security standards of the Gramm-Leach-Bliley Act (GLBA), they are not examined or supervised for their compliance with these standards in the same manner as financial institutions, yet they hold equally critical, personally sensitive information about consumers. This is a grave weakness that must be addressed in any data security legislation. 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 by the prudential financial regulators.

ICBA Lawsuit Against Equifax

ICBA and community bankers were appalled and troubled 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. In November 2017, ICBA filed suit in the U.S. District Court for the Northern District of Georgia to require Equifax to compensate all community banks harmed by the breach. The complaint cites the myriad damages caused by the breach, such as, for example, the costs of customer credit freezes, protective measures to deter and/or prevent fraud, and cancelation and replacement of payment cards. For a longer-term solution, ICBA also asks the court to require Equifax to improve its security infrastructure to prevent future data breaches.

Create Incentives to Strengthen Data Security

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

When a breach occurs at any point in the financial services chain, community banks take a variety of steps to protect the integrity of their customers' accounts, including, among other things, monitoring for indications of suspicious activity, changing customer identity procedures, responding to customer inquiries, reimbursing customers for confirmed fraudulent transactions, modifying customer limits to mitigate fraud losses, and blocking and reissuing payment cards of affected account holders at a cost to the community bank. Deposit account-holding and payment card-issuing banks repeatedly 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, not by the party protecting the consumer. 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.

Barring a shift in liability to the breached entity, community banks should continue to be able to access various cost recovery options after a breach.

A National Data Security Breach and Notification Standard is Vital

Many states have enacted laws with differing requirements for providing notice in the event of a data breach. This patchwork of state notification laws does not establish a uniform, baseline standard for the holders of sensitive data. A national notification standard is needed and should be accompanied by GLBA-like data security standards for all participants of the financial system to provide consumers a greater level of protection. This national data security standard should include various cost recovery options, including but not limited to a meaningful private enforcement mechanism. Federal banking agencies should continue to set the notification standard for financial institutions.

It is equally important that community banks receive timely notification concerning the nature and scope of any breach when bank customer information, such as account or payment card numbers, may have been compromised. Expeditious notification is critical to loss mitigation.

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.