March 7, 2018

DATA SECURITY LEGISLATIVE SOLUTIONS: 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 "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime." ICBA is pleased to have the opportunity to submit 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 is pleased to offer the community bank perspective on the two legislative proposals before this committee today.

THE "DATA ACQUISITION AND TECHNOLOGY ACCOUNTABILITY AND SECURITY ACT"

This discussion draft, offered by Chairman Luetkemeyer and Rep. Carolyn Maloney, would create a national data breach notification standard to replace the current patchwork of differing state breach notification laws. In an integrated national economy with a geographically mobile population, consistent standards and expectations are needed to avoid consumer confusion.

ICBA supports the security requirements in the discussion draft, which would subject other entities to a scalable data security standard. Community banks have long been subject to regulatory mandates that set rigorous data protection practices. These mandates are fundamental and a critical component of the safety and soundness of the overall banking system. With data breaches in the news almost daily, the status quo advocated by other sectors is simply not working for American consumers. Consumers demand that their personal information be held securely and not subject to innumerable breaches. The only way to achieve this objective is by raising the bar to ensure all entities are subject to comparable standards.

While ICBA is supportive of the discussion draft and the objectives it is attempting to achive, we respectfully recommend that the bill be strengthened by creating incentives for improved data security for all entities that hold, store, or process personally identifiable information by creating a legal structure in which the entity that incurs a breach – be it a retailer, credit reporting agency (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, notifying customers, 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. 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.

ICBA thanks Chairman Luetkemeyer and Rep. Maloney for crafting this proposal, and we look forward to working with them as it advances.

THE "PROMOTING RESPONSIBLE OVERSIGHT OF TRANSACTION AND EXAMINATIONS OF CREDIT TECHNOLOGY ACT OF 2017" (H.R. 4028)

H.R. 4028, sponsored by Rep. Patrick McHenry, would, among other things, subject the CRAs to examination and supervision by a banking regulator to be determined by the Federal Financial Institution Examinations Council (FFIEC). ICBA strongly supports Title I of this bill.

The massive data breach at Equifax, which exposed the personal data of 148 million American consumers and counting, shows the ongoing vulnerability of 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 in our current system. 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 thanks Rep. McHenry for introducing H.R. 4028 and we look forward to working with him as it advances through the legislative process.

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 enact laws that will promote customer security, protect against costly and damaging data breaches, and further enhance the safety and soundness of our financial system.