ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

December 10, 2014

Cybersecurity: The Community Bank Perspective

On behalf of the more than 6,500 community banks represented by the Independent Community Bankers of America (ICBA), thank you for convening today's hearing "Cybersecurity: Enhancing Coordination to Protect the Financial Sector." We welcome the opportunity to share the community bank perspective on this critical, dynamic issue.

The financial services industry and community banks are on the front lines of defending against cybersecurity threats and take their role in securing data and personal information very seriously. Community banks are strong guardians of the security and confidentiality of customer information as a matter of good business practice as well as legal and regulatory requirements. Safeguarding customer information is central to maintaining public trust and the key to long-term customer retention. As Congress, law enforcement and the regulatory agencies continue to address the real and present danger cybercriminals pose to the financial system, we ask that they keep in mind the following policy principles and objectives of the community banking industry:

Policymakers Must Recognize Existing Data Security Mandates and Close Remaining Gaps. Any new legislation, frameworks, or standards policymakers develop should first recognize the existing standards and practices community banks observe to protect the confidentiality and integrity of customer personal data as well as to mitigate cyber threats and then focus on closing remaining gaps. The National Institute for Standards and Technology (NIST) framework, for example, and the 2013 Executive Order implementing it, were developed to create a baseline to reduce cyber risk to all critical infrastructure sectors, and the Gramm-Leach-Bliley Act, sets forth rigorous and effective data security protocols for the financial sector. It is important to extend comparable standards to ALL critical infrastructure sectors, including the commercial facilities sector which incorporates the retail industry and other potentially vulnerable entities.

Threat Information Sharing is Critical. ICBA supports the sharing of advanced threat and attack data between federal agencies and the appropriate financial sector participants, including community banks. Community banks rely on this critical information to help them manage their cyber threats and protect their systems. ICBA supports community banks' involvement with services such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. ICBA also supports FS-ISAC efforts to take complex threat information across communities, people and devices and analyze, prioritize, and route it to users in real-time as long as those efforts incorporate community banks and such advancements are cost effective for them.

Additionally, ICBA supports the recent creation of the Retail Cyber Intelligence Sharing Center (R-CISC) and supports the establishment of robust information sharing protocols between the two sector ISACs.

Regulators Should Do More to Control Third Party Risk. Community banks significantly rely on third parties, such as data processing companies and software vendors, to support their systems and business activities. While community banks are diligent in their management of third parties, mitigating sophisticated cyber threats to these third parties, especially when they have connections to other institutions and servicers, can be challenging. Regulators should enhance their oversight of these third parties in order to mitigate the risks associated with interconnectivity and share threat and other applicable information with community banks on a timely basis.

ICBA Position on Recent Data Breaches

Community bankers and their customers are deeply alarmed by the wide-scale data breaches at national retail chains and other entities. These far-reaching and costly breaches have the potential to jeopardize consumers' financial integrity and confidence in the payments system.

To mitigate this risk, ICBA calls on policymakers to consider the following:

The Party that Incurs a Breach Should be Liable for Associated Costs. It is critical that the party that incurs a data breach, whether it be a retailer, financial institution, data processor or other entity, bear responsibility for the related fraud losses and costs of mitigation. Allocating financial responsibility with the party that is best positioned to secure consumer data will provide a strong incentive for it to do so effectively. Additionally, aligning incentives to maximize data security by all parties that process and/or store consumer data will make the payments system stronger over time. Payments rules should mandate merchant security provisions to further protect customer data, particularly debit and credit card information.

Extend Gramm-Leach-Bliley Act-Like Standards. Under current law, retailers and other parties that process or store consumer financial data are not subject to the same federal data security standards and oversight as financial institutions. Securing financial data at financial institutions is of limited value if it remains exposed at the point-of-sale and other processing points. ICBA supports subjecting these entities to Gramm-Leach-Bliley Act-like standards with similar enforcement. It is equally important that these entities provide uniform and timely notification to banks concerning the nature and scope of any breach when bank customer information may have been compromised.

A 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. ICBA believes customer notification is appropriate to let customers take steps to protect themselves from identity theft or fraud resulting from data breaches. However, it is important that notification requirements allow financial institutions and others flexibility to determine when notice is appropriate. Overly broad notification requirements defeat the purpose of calling attention to the risks associated with a particular breach. Federal banking agencies should set the standard for financial institutions, as they currently do.

Thank you again for the opportunity to submit this statement for the record. ICBA is committed to working with this committee to address cyber threats and data breaches brought by criminal enterprises.