ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

May 19, 2015

Cybersecurity: The Community Bank Perspective

On behalf of the more than 6,000 community banks represented by ICBA, thank you for convening today's hearing on "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats." The financial services industry and community banks are on the front lines of defending against cyber threats and take their role in securing data and personal information very seriously. ICBA is pleased to take this opportunity to submit the following statement for the record which sets forth the community bank perspective on cybersecurity.

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 and their third-party service providers rely on this critical information to help them manage their cyber threats and protect their systems. ICBA strongly supports H.R. 1731 and H.R. 1560, passed by the House in April, which would provide liability protection with regard to information sharing, while balancing the need to protect privacy. These bills will help foster a more robust cyber threat information sharing ecosystem.

ICBA also supports community banks' membership and 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 cyber threat and vulnerability information. ICBA also supports FS-ISAC efforts to gather complex threat information across communities, people and devices and analyze, prioritize, and route that information to users in real-time. These efforts must incorporate community banks and be cost effective for them.

All Critical Infrastructure Sectors Must Be Covered and Existing Mandates Must Be Recognized. ICBA supports the 2013 Executive Order and the NIST framework implementing it because they create a baseline to reduce cyber risk to all critical infrastructure sectors. This is a critical test for any new legislation, frameworks, or standards in the area of data security: It should extend comparable standards to all critical infrastructure sectors, including the commercial facilities sector which incorporates the retail industry and other potentially vulnerable entities. Financial institutions have long been subject to rigorous and effective data security protocols established by the Gramm-Leach-Bliley Act. Any new data security mandates must 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.

Regulators Should Recognize Third Party Risk. Community banks significantly rely on third-party service providers to support their systems and business activities. While community banks are diligent in their management of third-party service providers, mitigating sophisticated cyber threats to these providers can be challenging, especially when they are connected to other institutions and servicers. Regulators must be aware of the significant interconnectivity of these third-party service providers and collaborate with them in addressing cyber threats. Regulators should evaluate the concentration risks of service providers to financial institutions. In addition, the Multi-Regional Data Processing Servicer Program should be broadened to include more core, IT service providers.

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:

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.

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.

Data Security Act of 2015 (H.R. 2205) Strengthens Consumer Data Security

ICBA strongly supports H.R. 2205, introduced by Chairman Neugebauer and Representative Carney, which would extend Gramm-Leach-Bliley-like standards to all entities that handle sensitive consumer

data, without duplicating the standards that already apply to financial institutions. H.R. 2205 would also replace the current patchwork of state and federal regulations for data breaches with a national law that provides uniform protections across the country.

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.