ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

January 28, 2015

Cybersecurity: The Community Bank Perspective

On behalf of the more than 6,500 community banks represented by ICBA, thank you for convening today's hearing on "Protecting America from Cyber Attacks: The Importance of Information Sharing."
The financial services industry and community banks are typically on the front lines of defending against cybersecurity 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 information sharing and other aspects of 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 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 to community banks.

Policymakers Must Recognize Existing Data Security Mandates. 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. The Gramm-Leach-Bliley Act, for example, 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. The National Institute for Standards and Technology (NIST) framework, and the 2013 Executive Order implementing it, were developed to create a baseline to reduce cyber risk to all critical infrastructure sectors.

Regulators Should Recognize Third Party Risk. Community banks significantly rely on third parties 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 must be aware of the significant interconnectivity of these third parties and must collaborate with them to mitigate this risk. This can be done by agencies evaluating the concentration risks of service providers to financial institutions, and broadening supervision of technology service providers to include more core, IT service providers by expanding the Multi-Regional Data Processing Servicer Program (MDPS) to include such providers.

Properly Aligned Incentives Will Enhance Data Security and Cybersecurity. When an entity's systems are breached, it is critical that the party that incurs the 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 and cybersecurity by all parties that process and/or store consumer data will make the payments system stronger over time.

Thank you again for convening today's hearing. ICBA looks forward to working with the Senate Committee on Homeland Security and Governmental Affairs to improve cybersecurity.