INDEPENDENT COMMUNITY BANKERS of AMERICA®

JACK A. HARTINGS
Chairman
REBECA ROMERO RAINEY
Chairman-Elect
R. SCOTT HEITKAMP
Vice Chairman
PRESTON KENNEDY
Treasurer
J. MICHAEL ELLENBURG
Secretary
JOHN H. BUHRMASTER
Immediate Past Chairman

CAMDEN R. FINE
President and CEO

April 15, 2015

The Honorable Lynn Westmoreland
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Randy Neugebauer
U.S. House of Representatives
Washington, DC 20515

The Honorable David Scott
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Kyrsten Sinema
U.S. House of Representatives
Washington, DC 20515

Dear Representatives Westmoreland, Neugebauer, Scott, and Sinema:

On behalf of the more than 6,000 community banks represented by ICBA, I write to congratulate you for forming the Congressional Payments Technology Caucus (CPTC). The CPTC will provide a much-needed forum for the discussion of evolving payments technology issues, educating members of Congress, and evaluating legislative proposals. As you can appreciate, policy must keep pace with innovation to create a secure environment for payments, protect sensitive consumer data, and maintain confidence in the integrity of the payments system. The CPTC will play a critical role in ensuring that policy is current, flexible, and informed by the views of all payments system participants.

Community banks and community bank customers have a great deal at stake in the payments system. Cutting edge payments technology helps community banks remain competitive with larger banks. The viability of community banks creates a more diverse financial system, offering a broader choice of competitively-priced products and services for the benefit of consumers and small businesses.

To this end, we would welcome the opportunity to meet and share our perspectives on the payments system at your earliest convenience. In advance of such a meeting, please find below an outline of community bank priorities in the area of payments technology.

Data Security

Community banks are strong guardians of the security and confidentiality of customer information as a matter of good business practice and legal and regulatory requirements. Safeguarding customer information is central to maintaining public trust. Our principles for strengthening data security are:

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 best positioned to secure consumer data will provide a strong incentive for it to do so.

Extend Standards Similar to Gramm-Leach-Bliley. 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 standards similar to Gramm-Leach-Bliley Act with comparable enforcement.

A National Data Security Breach and Notification Standard. 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 timely notification is critical to allow customers take steps to protect themselves from identity theft or fraud resulting from data breaches. Notification requirements should 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 continue to set the standard for financial institutions.

New Technologies Will Reduce Risk But There Is No Single Universal Remedy. Community banks are already investing in technologies, including a migration to chip technology for debit and credit cards that will better secure transactions processing and thwart criminals. Even with these technologies in place, criminals will continue to try to find weaknesses in data security, so it is crucial the marketplace continue to have the flexibility to innovate.

Cybersecurity

The financial services industry and community banks are on the front lines of defending against cybersecurity threats. ICBA advocates the following principles for strengthening cybersecurity:

Policymakers Must Recognize Existing Data Security Mandates. Any new legislation, frameworks, or standards policymakers develop should 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 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. As mentioned above, 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.

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. The banking agencies should evaluate the concentration risks of service providers to financial institutions, and broaden 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.

Faster Payments

A faster payments system is critical to meeting the evolving payments needs of customers. ICBA strongly supports industry efforts toward faster payments and actively supports and participates in initiatives by the Federal Reserve Banks, NACHA and The Clearing House, ensuring coordination between these efforts. Core attributes of any faster payments system should include end-user payment experience, ubiquity, efficiency, inter-bank compensation and strong oversight by financial institutions.

The principles outlined above are the result of ongoing deliberations among a broad range of community banks with diverse business models and distinct roles in the payments system. The principles are intended to create a secure environment for payments with broad flexibility for continued marketplace innovation that will benefit customers and small businesses.

Virtual Currencies

Virtual currencies offer consumers a new choice of payment method and are spurring significant investments in payments technology that have the potential to create new options for consumers and investors in the future. However, current limited regulation and oversight applied to the virtual currency marketplace and transactions in virtual currency mean that consumers and investors that pay with or hold virtual currency are exposed to significant risks. A federal and state regulatory framework for virtual currencies would greatly reduce these risks.

We look forward to meeting with you to discuss these and additional issues in greater detail.

Sincerely,

/s/

Camden R. Fine
President & CEO