ICBA
INDEPENDENT COMMUNITY
BANKERS *of* AMERICA®

March 8, 2017

Countering Cyber Risk for Community Banks and Their Small Business Partners

On behalf of the more than 5,800 community banks represented by ICBA, we thank Chairman Chabot and Ranking Member Velazquez for convening today's hearing entitled: "Small Business Cybersecurity: Federal Resources and Coordination." This is a critical topic for community banks both as small businesses that hold sensitive customer data and as the primary lenders to small businesses. Community banks have a vested interest in small-business cybersecurity and prosperity. ICBA is pleased to have this opportunity to offer this statement for the record.

The Community Bank-Small Business Partnership

America's community banks are prolific small business lenders, playing an outsized role in funding small businesses and the jobs they create. While community banks represent 17 percent of all U.S. bank assets, they make more than half of all small business loans. Small businesses create nearly two-thirds of all new jobs in the United States and account for more than half of all employment.

Community Banks and Cybersecurity

Community banks are committed to safeguarding customer data and personal information. The community bank business model is founded on customer trust and service, and cybersecurity is a business imperative in the digital marketplace. Community banks invest significant and increasing resources in security controls to protect their individual data and critical systems.

Community banks adhere to existing law, regulation and guidance for protecting both bank and customer data. For example, the Federal Financial Institutions Examination Council ("FFIEC") Information Technology Examination Handbook ("IT Handbook") provides guidance and is the standard by which banks are examined based on operational resiliency, scope, risk, and complexity with regard to cybersecurity. All community banks are examined and supervised to ensure they comply with the requirements of the IT Handbook.

One of these requirements is to conduct a risk assessment. This is critical to any business entity that operates in today's modern technological environment. Risk assessments can be done by employing a variety of tools, frameworks, and assessments. Many of these have been developed by the private sector and include the Control Objectives for Information and Related Technology

("COBIT") and the SANS CIC Critical Security Controls. Others have been introduced for voluntary use by community banks, such as the FFIEC Cybersecurity Assessment Tool ("CAT"). There is also the NIST Cybersecurity Framework. With the exception of the IT Handbook, all of these tools, frameworks, and assessments are voluntary, and it is critical to community banks that they remain so.

It is not uncommon for community banks to employ parts of various voluntary frameworks, tools, and assessments to create a tailored cybersecurity program for their institution, based on the banks' risk, size, and scope. ICBA believes both Congress and the federal banking agencies should recognize this flexible approach to cybersecurity, and any new legislation or regulation must preserve this approach.

Data Security

Data breaches at national retail chains and elsewhere have the potential to jeopardize consumers' financial integrity and confidence in the payments system. 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 and retaining customers. However, bad actors will continue to look for weaknesses in the payments and information systems in various industries, and breaches will occur. ICBA supports the following to mitigate losses in the event of a breach:

- All participants in the payments system, including merchants, and all entities with access to customer financial information, should be subject to Gramm-Leach-Bliley Act-like data security standards.
- ICBA supports a national data security breach and notification standard to replace the current patchwork of state laws.
- Community banks should be notified of a potential and/or actual breach as expeditiously as possible in order to mitigate losses.
- The costs of data breaches should ultimately be borne by the party that incurs the breach. Barring a shift in liability to the breached entity, community banks should continue to be able to access various cost recovery options after a breach.
- Banks, card networks, and financial technology companies must continue to freely innovate to effectively protect consumer data and confidence.
- ICBA strongly supports ongoing regulatory efforts and existing, voluntary, public-private partnerships to address the growing threat of cyber-attacks.
- ICBA supports stronger data security standards for regulatory agencies and staff.

Payment Security

Payment card system stakeholders, including networks, merchants, card issuers, and cardholders, are concerned about growing security risks and the shift to more sophisticated and secure technology such as chip, tokenization, and end-to-end encryption. While chip cards, with or without PINs, are a step in the right direction in terms of data security, they are not a panacea. None of the major, recent data breaches at U.S. retailers were caused by customers using payment cards without PINs, and none of these breaches would have been prevented by customers using cards with PINs.

Re-engineering a payments system is not an easy task as there are many players that need to collaborate, from the card networks and processors to the bank issuers and merchants. ICBA is actively participating in this migration by conveying the community bank perspective to all stakeholders and communicating the implications of these changes to community banks and their customers.

Closing

Thank you again for convening this hearing and raising the profile of a critical topic for community banks and the small businesses they partner with. ICBA looks forward to continuing to work with the committee in our combined effort to better coordinate cybersecurity efforts, promote payments security, and protect against costly and damaging data breaches.