Statement of the Robert S. Nichols
President and Chief Executive Officer, Financial Services Forum

Testimony Before the
Subcommittee on Financial Institutions and Consumer Credit
of the
House Financial Services Committee

May 19, 2015

Introduction

Chairman Neugebauer, Ranking Member Clay, thank you for the opportunity to participate in today's hearing on the threat posed by cyber attacks to our financial system.

As you mentioned, I am here as President and Chief Executive Officer of the Financial Services Forum. The Forum is a financial and economic policy organization comprising the chief executive officers of 18 of the largest and most diversified financial institutions with operations in the United States. The Forum works to promote policies that enhance savings and investment, and that ensure an open, competitive and sound global financial services marketplace.

Mounting Threat of Cyber Attack

Today's hearing is both enormously important and remarkably timely. In recent years cyber attacks have grown rapidly, both in number and level of sophistication. According to Symantec Corporation, a leading information and Internet security firm, cyber attacks around the world soared 91 percent in 2013 alone.

Just last week, the Depository Trust & Clearing Corporation, a New-York-based securities settlement and clearing firm, released its Systemic Risk Barometer for the first quarter of 2015, based on a survey of financial market participants. Asked to identify the top risks to the financial system, respondents cited cyber attack as the number one threat, with respondents specifically noting the growth in the "frequency and sophistication of cyber-attacks."

As the sophistication and frequency of attacks has increased, so have the range of culprits. Unfriendly nation-states breach systems seeking intelligence or intellectual property. So-called "hacktivists" aim to make political statements through systems disruptions. And organized crime groups, cyber gangs, and other criminals breach systems for monetary gain. A growing black market for breached data further encourages such attacks.

In some cases, the attackers appear to be parts of state-sponsored cyber-espionage efforts. It should come as no surprise that North Korea chose to target the South Korean financial system's cyber-infrastructure. Just a few days ago on May 12th, *Politico* reported that sophisticated hackers, thought to have ties to the Kremlin, used malware to launch an attack on a number of large international financial institutions. Cyber attacks on financial institutions not only threaten the security of financial information belonging to American households and

businesses, but can also, potentially, threaten financial institutions themselves, financial stability, the broader economy, and, ultimately, our national security.

Financial Industry Cyber Defense Efforts

Effectively defending against the mounting threat of cyber attack requires resources, technical sophistication, and cooperation – among financial institutions and between the financial industry, other critical infrastructure sectors, and the relevant government agencies. Large financial institutions are working hard to deliver every day on each of these critical fronts.

In the same way that community banks have the local knowledge that positions them to service their communities in unique ways, large globally active financial institutions are positioned to play a crucial role in protecting not just their banks' customer information, but the financial system as a whole.

With regard to resources and technical expertise, large financial institutions remain at the cutting edge of cyber protection and are regarded by most experts – both in the private sector and in government – as having developed and deployed some of the most sophisticated and effective defenses against cyber attacks in the corporate world.

With regard to industry cooperation and coordination, cyber security in the financial sector is a team effort – because it has to be. To be successful, the industry must invest in, and operate within, a single unified cyber security culture. And we do. Working with our colleagues across the financial sector, large institutions continuously enhance the sector's capabilities, processes and procedures, and incorporate lessons learned from real incidents and exercises.

In particular, large financial institutions are investing in ever-more robust and automated systems of threat analysis and sharing. Automated threat analysis enables the quick and reliable differentiation of lower-level problems from more serious threats, allowing our cyber defense professionals to focus on more sophisticated and malicious activity. And automated sharing enables the swift dissemination of threat information across the financial system.

In other hearings before this Committee, some witnesses have questioned whether America needs large globally active financial institutions. Mr. Chairman, the U.S. economy is the largest and most complex economy in the world, with a highly diverse range of financial product and service needs. Meeting those diverse needs requires financial institutions of all sizes and business models.

In the cyber defense arena, it is often the largest institutions that have the resources, and that are making critical investments, to combat emerging threats as they proliferate and grow in frequency and sophistication. As difficult and expensive as it is to build and maintain a robust cyber defense network, making major changes to those networks – due to forced divestitures or other major structural changes at financial institutions – would entail significant risks, including: overall network defense during and after the transition, the potential loss of top firm talent, and potential loss of intellectual property of home grown cyber security solutions.

Industry-Government Cooperation Critical

Cooperation between industry and government is also vital if the battle against mounting cyber threats is to be won. To date, cooperation with the relevant government agencies has been good, but can and must be much better. In particular, industry efforts regarding threat assessment and information sharing are constrained by lingering fear of legal liability and potential exposure, even if cyber threat information is shared in good faith and for appropriate defense purposes.

To effectively combat the mounting threat of cyber attack, financial institutions – again, widely regarded as the most sophisticated and effective defenders against cyber attacks in the corporate world – should not have to worry when sharing threat information with law enforcement, regulatory agencies, the Department of Homeland Security, or the Treasury Department. Such concerns leave financial institutions unnecessarily exposed to operational and reputational risks, undermining the cyber defense efforts in which industry and government have a pronounced mutual interest.

To encourage better cyber threat information sharing within the financial sector, and between industry and government, legislation providing sensible "Good Samaritan" protections is needed. Such legislation should:

- Facilitate real-time cyber threat information sharing to enable financial institutions and government to act quickly;

- Provide liability protection for good faith cyber threat information sharing;

- Provide targeted protections from public disclosures, such as exemptions from certain Freedom of Information Act requests;

- Facilitate appropriate declassification of pertinent government-generated cyber threat information and expedite issuance of clearances to selected and approved industry executives; and,

- Include appropriate levels of privacy protections.

With these needs in mind, the bill passed by the House on April 22nd is a major and important step forward, and will greatly facilitate industry's continued cooperation with government. We hope the Senate will soon take up its information sharing proposal to continue progress on this important issue. We urge swift movement and passage on this important legislation.

Conclusion

Chairman Neugebauer, cyber attacks on our nation's financial institutions and financial system are a regrettable fact of life in the digital age – one that can only be expected to spread and intensify in the future. Fortunately, America's financial institutions and, in particular, large financial institutions, continue to develop and deploy state-of-the-art corporate cyber defense tools, methods, and systems. But we cannot win this fight alone. For America's financial system to effectively anticipate, protect against, and respond to cyber threats, government – and industry's undeterred cooperation with government – is essential.

As financial institutions, data and information are the tools we work with and no issue is of higher priority than protecting our customers, their savings, and their financial information. Large institutions know that the bad guys are going to continue to find new and innovative ways to attack the network and systems that we fight to protect. But we will be able to be nimble in response if we can do a couple of things well:

1) Find, maintain and develop talented cyber-security experts in the financial sector;

2) Focus on good crisis management preparation and operational preparedness which increases speed to recovery; and,

3) Continue to work in partnership with the government entities and others across the financial system to share information to enhance security.

On behalf of the Financial Services Forum and its members, I commend you and Ranking Member Clay for your attention to this critical issue. We look forward to working with you to ensure that America's financial system, institutions, households, and businesses receive the protection that they need and deserve.