Testimony of

Doug Johnson

On behalf of the

New York Bankers Association

before the

New York State Senate Joint Public Hearing:

"Cybersecurity: Defending New York from Cyber Attacks"

November 18, 2013

NYBA

American Bankers Association

Testimony of
Doug Johnson
On behalf of the
New York Bankers Association
Before the
New York State Senate Joint Public Hearing:
"Cybersecurity: Defending New York from Cyber Attacks"
November 18, 2013

Chairmen Griffo, Seward, Ball, Valesky, Gallivan and Golden, my name is Doug Johnson, Vice President and Senior Advisor, Risk Management Policy for the American Bankers Association. In that capacity, I currently lead the ABA's enterprise risk, physical and cyber security, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership. I am also the current Vice Chairman of the Financial Services Sector Coordinating Council, which advises the federal bank regulatory agencies on homeland security and critical infrastructure protection issues; as well as a board member of the Financial Services Information Sharing and Analysis Center, a private corporation that works with government to provide the financial sector with cyber and physical threat and vulnerability information as part of the nation's homeland security and critical infrastructure protection efforts.

I appreciate the opportunity to be here today representing the New York Bankers Association. In my testimony, I will discuss the nature of the cyber threat we face, both as an industry and as a country, and how our sector is organized and regulated to actively address that threat. I will also describe the actions that are underway at the Federal level to enhance cybersecurity, and close with how New York State can continue to play a leadership role in our nation's cybersecurity efforts.

I. The Cyber Threat is Real and Growing

As you are aware, our nation's financial sector experienced a large number of cyber-attacks during 2013, mostly in the form of distributed denial of service, or DDoS attacks. These attacks

were largely designed to disrupt our sector's customer-facing online banking platforms, causing periodic loss of availability for those customers. They did not compromise the privacy of customer information or the integrity of bank systems. They were, however, large sustained attacks that challenged the resources of the money center, regional, and community banks that were targeted.

Many of our efforts in the financial services sector are to ensure that attacks designed to disrupt users do not set the stage for data compromises or attacks on system integrity. We have seen some instances of blended attacks, where DDoS traffic is used as a diversion from a simultaneous attack on high value customers. We are also aware that a DDoS attack can also be an attempt to test various points of entry within a financial institution's system for later, more sophisticated attacks. We are always alert for these possibilities. And we expect the nature of attacks to change over time, continuing to increase in sophistication and strength.

Our sector is also mindful of attacks that have occurred overseas which, if conducted against U.S. financial institutions, could have significant impact on systems and customers. The attack on Aramco Oil in August of 2012, where an insider distributed a computer virus called Shamoon wiped the data off approximately 30,000 computers, and the attacks against South Korean banks, purportedly by North Korea, that shut down ATM systems for several hours and disabled over 3,000 computers. These are just two examples of the types of attacks necessitating a high level of readiness on the part of our government and industries.

We are also aware that our vulnerability to such attacks are in many instances based on security gaps that may exist on the part of our retail and business customers, outsourced service providers, or other business partners. The irony is that within the army of computers that bombard a bank's online banking platform with traffic during a denial of service attack may be compromised computers of that bank's customers. Many financial institutions, particularly those that are community-based, are also highly dependent on core banking system processors and internet banking service providers for cybersecurity protection. It is thus important that we strive to protect the entire financial ecosystem, and ensure that our critical service providers abide by the same cybersecurity requirements that the financial institutions must adhere to, as a regulatory requirement but also as a business imperative.

II. The Financial Sector is Actively Addressing the Cyber Threat

The nature and frequency of the recent cyber-attacks has focused a great deal of financial institution attention on whether their institutions, regardless of size, are properly prepared for such events, and whether the appropriate level of resources are being expended both as a sector and as institutions to detect and defend against them. Attention has also been directed toward whether the financial sector is organized appropriately to detect and respond to future attacks and whether government is an active and engaged partner in our efforts. These efforts build on long-standing, collaborative efforts on the part of the financial sector to protect institutions and customers from physical as well as cyber events. A significant protection infrastructure, in partnership with government, exists and is continually being improved.

As I have already indicated, in addition to my role at ABA, I am proud to currently serve as the Vice Chairman of the Financial Services Sector Coordinating Council (FSSCC). I am also on the board of its sister organization, the Financial Services Information Sharing and Analysis Center (FS-ISAC). We have been deeply involved in and supportive of these two organizations since their inception.

Established in 2002, FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, and collaborating with the U.S. government. The Council has 60 volunteer member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms. During the past decade the partnership has continued to grow, both in terms of the size and commitment of its membership as well as the breadth of issues it addresses. Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of financial consumers and the nation.

The FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive - later updated by 2003's Homeland Security Presidential Directive 7 - mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical

infrastructure. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC is positioned to quickly disseminate physical and cyber threat alerts and other critical information throughout the financial sector. The FS-ISAC has also recently taken over the role of coordinating crisis response for the sector, formerly a responsibility of FSSCC.

Our government partner in these efforts is the Financial and Banking Information Infrastructure Committee, or FBIIC, which is led by Treasury and chartered under the President's Working Group on Financial Markets. FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Essential to the FSSCC's success is the public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime.

The deep involvement of ABA in both the FSSCC and the FS-ISAC is not unusual within the financial services sector. Many financial organizations are heavily involved in both. And this collaboration does not include only the largest financial organizations. Our diverse sector is made up of organizations of all sizes and types. ABA has been a primary driver behind expanding the FS-ISAC's reach from under 100 to over 4,000 members to ensure that vital cyber threat information, and the means to defeat those threats, reaches as many financial organizations as possible.

New York financial institutions have always played a leadership role within these two organizations, and indeed were the founding members of the FS-ISAC. Currently, the Managing Director Global Head of Information Security of Citi, Charles Blauner, and JP Morgan Chase's Chief Information Risk Officer, Anish Bhimani, respectively serve as the chairs of the FSSCC and the FS-ISAC.

The financial services sector develops and implements leading practices through the FSSCC, the FS-ISAC and the FBIIC. For example, under the joint partnership of the FSSCC and FBIIC, our sector has developed leading practices to mitigate risks associated with the resiliency of the telecommunications infrastructure including critical undersea cables, pandemic flu preparations, and other important risks or threats facing the security and resilience of the sector.

The most recent example of the high degree of interaction and collaboration between these bodies is of course our sector's unified response to the recent DDoS attacks that have occurred since September, 2012. As the number of affected organizations increased, the FS-ISAC was able to organize them into a group to collaborate on measures to mitigate the attacks. Individual organizations were able to, through FBIIC and Treasury, request specific governmental technical assistance as necessary. Due to the tight relationship between the FS-ISAC and the FSSCC, actions such as these are factored into the actions taken by the FSSCC as the Council makes and refines legislative and administrative policy recommendations.

The financial sector's response to Superstorm Sandy is another example of effective collaboration. Prior, during, and after the storm, the FS-ISAC and the FSSCC organized a large number of calls for the sector with New York and New Jersey emergency management personnel, Treasury, and DHS to ensure that financial services were available to those within the affected areas as soon as possible. As such events are inherently local, the New York and New Jersey state bankers associations were vital components of the recovery as we ensured that cash was distributed where it was most needed and that we had an accurate picture of where broader financial services were available.

III. Federal Action is Needed to Further Improve Cybersecurity

It is our sector's view that, given the escalating nature of the cybersecurity threat, further Federal action is necessary to properly address that threat. ABA continues to support the goals of the Administration and Congress to limit cybersecurity threats to business, our government, and the American people.[1]

As Congress and the Administration contemplate changes to the national cybersecurity framework, in addition to considering the cybersecurity measures our sector currently takes collaboratively, also important are the stringent laws and regulations within the financial services sector. Our sector is subject to a wide variety of federal and state laws, regulations, guidance, and examination standards relating to cybersecurity, many of which emanate from the general financial safety and soundness standards and customer information security provisions contained

[1] The FSSCC Comment Letter in Response to the NIST Request for Information, "Developing a Framework to Improve Infrastructure Cybersecurity" is available here: http://csrc.nist.gov/cyberframework/rfi_comments/040813_fsscc.pdf.

within the Gramm-Leach-Bliley Act of 1999. For example, financial institutions must comply with guidance produced by the Federal Financial Institution Examination Council (FFIEC). This guidance sets the standards for financial institution's information systems, outlining the minimum control requirements and directing a layered approach to managing information risks.

Likewise, the Securities and Exchange Commission (SEC) and the self -regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), and the National Futures Association (NFA) review the cybersecurity programs of exchanges, broker-dealers and clearing organizations as part of their ongoing supervisory exams and related activities. Insurance companies' privacy and security programs are subject to review by state insurance regulators.

We applaud the release of the Administration's recent Cybersecurity Executive Order and believe implementation of the Cybersecurity Framework envisioned in the Order can be an important tool in improving our nation's overall cybersecurity. Collaboratively, through the FSSCC, ABA is committed to working toward formulating and implementing this Framework in a manner that:

- ✓ Develops sector-specific frameworks recognizing the unique nature of and levels of protection within each critical sector;
- ✓ Ensures that each sector's primary regulatory authorities remain independent as the overseer and enforcement body for the critical sectors they regulate;
- ✓ Leverages existing audit and examination processes, encourages complementary, not redundant audit requirements when building voluntary cybersecurity practices, and;
- ✓ Creates incentives that are tailored to address specific market gaps.

Even considering the implementation of the Executive Order and the Cybersecurity Framework it envisions, the progress we are making is ultimately inadequate without Congressional action to enhance, facilitate, and protect threat information sharing across sectors and with government.

It is for this reason that ABA and NYBA supports the House passage of the Cyber Intelligence Sharing and Protection Act. The timely, voluntary sharing of threat information is critical to the government and the private sector in developing and deploying protective

measures against malicious cyber activity. While the cyber threat data that is shared by the financial services sector is machine language and not attributable to an individual, the provisions in the Act concerning liability protections for the sharing of information are also extremely important and transcend our sector. This legislation provides important clarifications that will help facilitate increased cyber intelligence information sharing between the private and public sectors.

Last week, the ABA, the Financial Services Roundtable, and the Securities Industry and Financial Markets Association sent a joint letter to Chairman Dianne Feinstein and Ranking Member Saxby Chambliss of the Senate Select Committee on Intelligence, indicating our support for the Committee's efforts to develop legislation that further strengthens the ability of the private sector and the Federal government to work together to develop a more effective information sharing framework to respond to cyber threats and providing liability protections while balancing the need for privacy protection. We are committed to continuing to work with Congress as it debates policies to strengthen our nation's cyber defense.

IV. New York State Has an Important Cybersecurity Role

New York will continue to play a leading role as we move forward collectively to improve our cybersecurity environment. National and state efforts must be complementary if we are to be successful, and there are a number of current initiatives underway in the states that meet that test.

New York City received the 2012 City Government Cybersecurity Leadership and Innovation Award from the Center for Digital Government for the development of an information security cloud implemented in 48 agencies. As a result of this initiative the city now has direct visibility into over 73,000 endpoints and serves as a model for securing government databases.

The recent establishment of the Governor's Cyber Advisory Board, designed to work with the administration on innovative strategies to keep New Yorkers safe from cyber threats and make recommendations for protecting the state's critical infrastructure and information systems, is another important development.

Cyber innovation closer to the location of this hearing is in the form of the CYBER NY Alliance and its associated New York State Cyber Research Institute (CRI). A primary focus

area of the CRI will be sensitive and classified cyber security research and development, designed to develop solutions to defend the safety, security and stability of our critical state and local infrastructures. Investments in such R&D initiatives should be encouraged, and we are supportive of any Congressional action at the Federal level that enhances tax and other incentives for cybersecurity research and development.

V. Conclusion

Thank you for holding this important hearing. Banks and other financial services companies have made cybersecurity a top priority. We have invested an enormous amount of time, energy and money to put in place the highest level of security among critical sectors, and we are subject to the most stringent regulatory requirements. We look forward to continuing to work with you toward our mutual goal of protecting our nation's critical assets.