Testimony of

Wm. Douglas Johnson

On behalf of the

American Bankers Association

before the

Subcommittee on Information Technology

of the

Committee on Oversight and Government Reform

United States House of Representatives

Testimony of

Wm. Douglas Johnson

On behalf of the

American Bankers Association

before the

Subcommittee on Information Technology

of the

Committee on Oversight and Government Reform

United States Senate

Wednesday, March 18, 2015

Chairman Hurd, Ranking Member Kelly, members of the subcommittee, my name is Doug Johnson, Senior Vice President, Payments and Cybersecurity Policy, of the American Bankers Association (ABA). In that capacity, I currently lead the association's physical and cybersecurity, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership.

I appreciate the opportunity to be here to represent the ABA and discuss the importance of instituting a uniform federal data breach law in place of disparate state laws. The ABA is the voice of the nation's $15 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $11 trillion in deposits and extend over $8 trillion in loans.

I also currently serve as Vice Chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and on the Board of Directors of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Established in 2002, the FSSCC is the national critical infrastructure protection coordinator for the financial sector, focused on operational risks. Because the FSSCC fits into a larger network of sector coordinating councils, it is uniquely positioned as the leader within financial services for developing strategies to improve shared critical infrastructure and homeland security.

Established in 1999, the FS-ISAC is the designated operational arm of the FSSCC. The Center supports the protection of the global financial services sector by assisting FSSCC, Treasury as well as regional agencies and entities to identify, prioritize and coordinate the protection of critical financial services, infrastructure service and key resources. The FS-ISAC also facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices.

As the 114th Congress engages in public debate on the important issue of cybersecurity, we share your concerns regarding the evolving nature of cyber threats facing the private sector. The ABA, now through its Center for Payments and Cybersecurity Policy, has historically been very supportive of these collaborative efforts to protect our sector's and nation's cybersecurity. The financial sector is an acknowledged leader in defending against cyber threats. These efforts, in their sixteenth year, are highly mature and increasingly focused on international and cross-sectorial efforts to enhance our collective ability to defend against and respond to cybersecurity attacks. We support effective cyber security policy and will continue to work with Congress to achieve that goal.

In my testimony I will focus on three main points:

- **The evolving nature of cyber threats.**
- **The role of technology in addressing cyber threats.**
- **The role of expanded information sharing in protecting against these threats.**

I. The Evolving Nature of Cyber Threats

According to the recently released "Worldwide Threat Assessment of the US Intelligence Community," while cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact, and the range of cyber threat actors, methods of attack, targeted systems, and victims are also expanding, the likelihood of a catastrophic attack from any particular actor is remote at this time. This highlights the persistent and ever-changing nature of the threats the private sector faces and will face in the future.[1]

Attacks that once were singular in focus, be it a denial of service attack on financial institutions, an attack against merchant point-of-sale devices, or an attempt to destroy or wipe data of an energy company, may now contain a variety of such attack vectors. Such multi-faceted attacks create particular challenges for the victimized company or companies, necessitating the simultaneous maintenance of availability, integrity, and confidentiality of data when formerly a cyber-attack might have impact on only one of these vital data security components.

Attackers of every variety are also becoming increasingly adept at defeating security practices, increasing the velocity with which companies must move to ensure they understand how cyber risks are changing and what mitigating measures are most effective against these risks. It is indeed an arms race.

Another increasing challenge for financial institutions and the private sector generally is the need to digest an increasingly larger volume of cyber threat data. Determining the relevance of a particular piece of threat data, analyzing the magnitude of the threat, evaluating which systems might be impacted, and devising the appropriate course to take to mitigate the threat if necessary has become increasingly difficult.

Lastly, the victim of the attack is also changing. Prior to 2014, much of the private and public sector cyber security focus was on critical infrastructure and the payments system. Now there is recognition that, given the broader motivations of attackers for conducting a cyber-attack, essentially any company and any sector could be subject to a significant, highly visible attack.

[1] Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, James R. Clapper, Director of National Intelligence, February 26, 2015, available at: http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

II. The Role of Technology in Addressing Cyber Threats

Technology obviously has a significant role in protecting our nation's companies and consumers from cyber threats. I would like to focus on two areas pertinent to today's hearing: technology used within our payment system and within our cyber threat information sharing environment.

The fact that attackers are becoming increasingly adept at defeating cybersecurity practices and mitigating measures points to the need for industry to develop and deploy enhanced measures on an ongoing basis with greater speed.

From the payment card technology standpoint, there is currently much discussion of the current roll-out of chip, or EMV payment card technology both at the point-of-sale and on the card itself. EMV technology consists of a small microprocessor chip embedded in a payment card, that an EMV-enabled point-of-sale device at a merchant can read, that encrypts card information. Utilizing EMV technology makes breached card data virtually useless to criminals wanting to replicate a card and use it physically at a merchant location. EMV technology does not, however, protect the card from being used online for purchases. A static card number, when compromised, could still be used for an unauthorized online purchase even if a chip was on the card.

Eliminating the use of static numbers altogether for debit and credit card purchases is a very important next step in protecting our payment system and the consumers that use it. Finding ways to keep consumers from having to remember static numbers, letters or symbols in order to authenticate themselves when conducting a financial or other sensitive transaction was a primary focus at the recent White House Summit on Cybersecurity and Consumer Protection. For instance:

- **Ajay Banga, President and CEO, MasterCard:** "What I have learned from my consumer customers is that they want two clear things aside from safety and security – one is to stop making me remember things to prove I am who I am. Because there are too many things to remember."[2]

[2] Ajay Banga, President and CEO, MasterCard, Remarks at The White House Summit Cybersecurity and Consumer Protection, Stanford University, February 13, 2015, available at: http://youtu.be/fleThSpCL.

- **Richard Davis, Chairman and CEO, US Bank:** “Our job is really a lot of financial literacy to help people understand how to protect themselves better…not putting a piece of tape on the back of your debit card or credit card and writing your PIN on it.”[3]
- **Chuck Scharf, CEO, Visa:** We can talk all we want about methods of authentication…but the fact is if card numbers are flying around even though there is zero liability it’s not something the consumer wants to go through…We are working with people across the payment ecosystem to figure out where we can get rid of those account numbers, so if there is a compromise, which there always will be because the bad guys are steps ahead as hard as we all try, the compromise does not have the effect it has today.”[4]

These comments point to the fact that payment security is a dynamic challenge that requires a like response, and that there is no single solution that will eliminate payment fraud. Locking in ***any*** static technology provides a roadmap to attackers, telling them where to focus their attacks. While payment networks, financial institutions, and merchants are all working toward installing chip technology prior to the October 2015 deadline, we are already seeing a migration of fraud to online, card not present transactions that chip technology cannot address, but tokenization can. Tokenization replaces sensitive consumer account information at the register or online with a random “token,” rendering any static information associated with the transaction useless to criminals, and thus shows great promise.

Another technological area that shows great promise is the FS-ISAC effort to automate the analysis and distribution of cyber threat data to the greatest extent possible. As I have already noted, the significant amount of threat information now being received by financial institutions has created increased difficulty in determining the relevance of a particular piece of threat data. There is a real danger, as our sector expands our information sharing capabilities to an increasing number of smaller financial institutions and outside the financial sector, that the sheer volume of threat information creates an unintended barrier to effective participation in threat information sharing.

[3] Richard Davis, Chairman and CEO, US Bank, Remarks at The White House Summit Cybersecurity and Consumer Protection, Stanford University, February 13, 2015, available at: http://youtu.be/KNny0o2o-pc.

[4] Chuck Scharf, CEO**, Visa**, Remarks at The White House Summit Cybersecurity and Consumer Protection, Stanford University, February 13, 2015, available at: http://youtu.be/jo_I6V-H8Xs.

To counteract this possibility, the FS-ISAC in concert with the Depository Trust and Clearing Corporation established Soltra, a strategic joint venture formed to utilize two new standards, Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXI) to develop an automated mechanism to receive and send cyber threat information machine to machine and dramatically reduce the effort and workload associated with threat intelligence.

The mechanism, called Soltra Edge, is able to automatically read and categorize threat indicators through STIX and then transmit them computer to computer via TAXI. While the Soltra Edge is currently used predominately by larger financial institutions, the system has recently been made available to smaller financial institutions free of charge. We also expect this solution to be adopted broadly by many critical sectors such as healthcare, energy, transportation, and retail.

The deployment of STIX and TAXI through the FS-ISAC is an excellent example of a set of standards initially developed by MITRE and the Department of Homeland Security (DHS) that now have an important commercial application that will greatly benefit the overall cybersecurity posture of our nation.

III. The Role of Expanded Information Sharing in Protecting against Cyber Threats

Recent cyber-attacks underscore the need to help ***all*** businesses improve their awareness of threats and enhance their response capabilities. The steps taken by the Administration, through the issuance of the February 13, 2015, executive order promoting private sector cybersecurity information sharing, will help the business community and government agencies share critical threat information more effectively.

While the recent executive order is an important step towards more effective information sharing, it is widely recognized that Congress must also act to pass legislation to fill important gaps that executive action cannot fill. For instance, legislation is necessary to give businesses legal certainty that they have safe harbor against frivolous lawsuits when voluntarily sharing and receiving threat indicators and countermeasures in real time and taking actions to mitigate cyberattacks. Legislation also needs to offer protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among public and private entities. ABA also believes that legislation needs to safeguard privacy and civil liberties and establish appropriate roles for civilian and intelligence agencies. The financial sector is dedicated to protecting customer data, and has led the way for effective information sharing through the development of the FS-ISAC. We are committed to working with others within the overall business community to develop a similarly strong and effective mechanism for sharing threat information.

I will focus on two important areas within the executive order: the acceleration of the DHS security clearance process and the establishment of Information Sharing and Analysis Organizations (ISAOs).

Information sharing is of critical importance to the financial services sector, other critical infrastructure sectors and the government. Without it, none of the financial sector's security and resiliency priorities would be achievable. With key federal support from the Treasury Department as our Sector Specific Agency, law enforcement and DHS, our network defenders are better able to prepare for cyber threats when there is a consistent, reliable and sustainable flow of actionable cybersecurity information and analysis, at both a classified and unclassified level.

As a nation, we are making some progress toward this goal, but it has become increasingly necessary for appropriately-cleared representatives of critical sectors such as financial services to have access, and provide contributions, to classified information that enables analysts and operators to take timely action to defend essential systems. Accordingly, the executive order's enhancement of DHS's role in accelerating the security clearance process for critical sector owners and operators is a clear indication of the Administration's support for this public-private partnership.

The ISAC's have played an important role for critical infrastructure protection information sharing and incident response for their sectors. The FS-ISAC, in particular, enjoys strong support from sector members, Treasury and DHS. In this spirit, we also support the creation of ISAOs as a mechanism for all sectors, regions and other stakeholder groups to share cybersecurity information and coordinate analysis and response. While ISACs must retain their status as the government's primary critical infrastructure partners, given their mandate for broad sectoral representation, the development of ISAOs should be facilitated for stakeholder groups that require a collaborative cyber and physical threat information sharing capability that builds on the strong foundation laid by the ISACs.

As the ISAO standards development process unfolds, certain principles must be upheld for structuring both the ISAOs themselves and the government's interaction with them:

- Sharing of sensitive security information within and among communities of trust is successful when operational standards of practice establish clear and enforced information handling rules;
- Information sharing is not a competitive sport: while competition in innovation can improve technical capabilities, operational standards should incentivize federated information sharing. Threat and vulnerability intelligence needs to be fused across trust communities, not diffused or siloed;
- Government internal processes for collecting, analyzing and packaging critical infrastructure protection intelligence for ISAC/ISAO consumption must be streamlined and transparent to maximize timeliness, accuracy and relevance of actionable shared information; and
- To manage scarce resources, government information sharing mechanisms such as the National Cyber and Communications Integration Center (NCCIC) and the Treasury Department's Cyber Intelligence Group (CIG) should prioritize engagements with ISACs and ISAOs according to transparently established criteria.

It is also important that the process to develop the ISAO standards is collaborative, open, and transparent. The process managed by the National Institute of Standards and Technology (NIST) during the development of the NIST Cybersecurity Framework is an excellent example of the appropriate leveraging of private sector input, knowledge and experience to develop guidance that will primarily impact non-governmental entities. We encourage DHS, as the implementing authority of the president's EO, to emulate the engagement model that NIST used to create and adopt their Cybersecurity Framework. The process worked.

Finally, for DHS to be successful implementing the EO and its many cyber security risk management and partnership authorities, it must be sufficiently resourced with the best analytical and technical capabilities, with a cadre of highly qualified cybersecurity leaders and analytical teams to conduct its mission. There must be a concerted effort to recruit, retain and maintain a world class workforce that is able to assess cyber threats globally and help the private sector reduce risk to this nation. With the application of the principles discussed in this statement, we believe the creation of ISAOs and their partnership agreements with DHS have the potential to complement the ISAC foundation and measurably improve cyber risk reduction for critical infrastructure and the national economy.

IV. The Path Forward

We look forward to working with Congress, the Administration and DHS to leverage the FS-ISAC as a successful model in the development of regional information sharing and analysis organizations. Above all, we urge Congress to send a bill to the president that gives businesses the liability and antitrust protections, and our citizens the privacy and civil liberty protections that will enhance our already significant efforts to protect the cybersecurity of our nation.