FINANCIAL SERVICES ROUNDTABLE

TESTIMONY OF TIM PAWLENTY

Chief Executive Officer, The Financial Services Roundtable

Committee on Homeland Security and Government Affairs

Hearing entitled

"Data Breach on the Rise: Protecting Personal Information from Harm"

April 2, 2014

342 Dirksen Senate Office Building

Chairman Carper, Ranking Member Coburn, Members of the Committee, thank you for this opportunity to appear before you today to address the important topic of data breaches and the further steps needed to better protect personal information and the payment system from cyber threats.

The Financial Services Roundtable (FSR) is a trade association representing the full range of the country's largest financial service companies. Our members include leading banking, insurance, asset management, finance and payment companies.

Cyber security has been a key focus area for FSR and our companies for decades. Since 1996, "BITS" -- the technology policy division of FSR, has played an important leadership role in cyber security, fraud reduction, vendor management, payments and emerging technologies.

Cyber risk is increasing in pace, complexity and potential impact. The threat has expanded from fraudsters committing financial theft to *hacktivists* causing disruptions and nation states threatening serious data manipulation and destruction. Cyber risk affects all institutions in our sector – large and small, banks, credit unions, insurers and investment firms.

Like everyone here, we were dismayed by the scale and scope of the recent data breaches at respected merchants and retailers. It is an indication of how cyber threats have intensified in recent years. It also represents an important opportunity for the financial services sector to partner with the merchant and retailer sector to mitigate cybersecurity threats and better protect customers in the broader payments ecosystems.

A recent *Washington Post* report suggested that over 3,000 companies were alerted to data breaches by federal agents in 2013. Even more disturbing, most of the companies did not even know they were breached. And this number only represents the number of cases in which federal agents were aware an attack occurred. A recent National Intelligence Assessment, cited by the *Washington Post*, concluded massive cyber-attack campaigns are ongoing and mostly generated from abroad.

The financial services sector is better prepared than other sectors to defend against and respond to cyber attacks. Individual financial institutions have and continue to invest substantial resources in personnel, products and services to defend themselves. We have one of the strongest private information sharing process of any critical infrastructure sector through our Financial Sector Information Sharing and Analysis Center (FS-ISAC), and we have been active supporters of our sector coordinating council – the Financial Services Sector Coordinating Council. Industry-wide initiatives are under way to identify and take action on information sharing, tactical operations, and investments in research and development. We plan and run simulations to improve our defenses and resiliency.

Financial institutions are also regulated and are examined to ensure compliance with comprehensive data security, privacy protection, vendor management and resiliency requirements. Over the past 15 months, the financial services sector has worked closely with the Treasury Department, regulators and other government agencies to improve cyber defenses. One example of these efforts is our involvement in the development of a cybersecurity framework for

critical infrastructure entities outlined in the President's Executive Order and Policy Directive on cyber security released in February 2013.

But we live in a networked world where the payment system is interconnected and all parts of the chain must have robust cybersecurity.

The implications of recent data breaches are profound, and they raise questions about cyber responsibility, new technologies, relationship between retailers and credit card companies (issuers and networks), technology standards, and many other issues.

These issues are incredibly important to FSR members and Sandy's members as well. So, about a month and a half ago, our teams got together to chart a course for working together to tackle these issues.

We established the Merchant and Financial Services Cybersecurity Partnership. The Partnership's mission is to work collaboratively across the payments system to enhance security to better protect customers and their data from cyber threats. Our goals include improving overall security across the payments ecosystem and to bolster consumer confidence in the security of their payment data and the systems used to process payments.

On February 27, Sandy and I convened the first meeting of the Partnership's Advisory Council which consists of 18 CEOs of major financial services and merchants/retailers trade associations. We decided to focus on five key areas and we then reached-out to executives from our member companies to serve on five working groups. We have strong participation from all key sectors of our industries and our working groups will begin their work shortly. Our five working groups are focused on the following topics:

- Threat information sharing,
- Cybersecurity risk mitigation,
- Advanced card present security technology,
- Card not present and mobile security, and
- Cybersecurity and data breach notification.

I would like to briefly discuss each of these areas.

Threat Information Sharing

The Threat Information Sharing working group will focus upon the capacity to share information regarding cyber threats and vulnerabilities within and between the retail and financial services industries. Both the retail and financial services industries must facilitate analysis and share threat information that identifies potentially fraudulent activities in its earliest stages. Doing so will bolster our ability to identify, thwart, and defend against attacks.

To accomplish this objective, we will explore options for inter-industry threat information sharing. This may include coordination with National Cyber Forensics Training Alliance (NCFTA), the Financial Services Information Sharing and Analysis Center (FS-ISAC) and other information sharing models and prospective partnerships. Existing information sharing avenues must be fully leveraged by both the financial services sector and retailers. We must also identify additional ways to facilitate threat information between the private and public sector.

Cybersecurity Risk Mitigation

The Cybersecurity Risk Mitigation Working Group will facilitate discussions with key stakeholders in the retail and financial services space on cyber risk mitigation and explore new technologies that allow us to better protect consumers.

Many of our member companies have effective technologies and practices in place to mitigate cyber risk. Although we must always be developing better technology and practices, progress can also be made by having industry leaders share best practice information with industry colleagues. This is especially important for smaller institutions that may not have the experience or resources to easily develop robust cyber security techniques.

Advanced Card Present Security Technology

The Advanced Card Present Security Technology Working Group will identify areas to improve technology in the card present payments ecosystem. We seek to enhance and better protect the security of the data, and to render any stolen data useless.

The specifics are still being developed, but some areas under consideration include: end-to-end data encryption; tokenization; a roadmap to move beyond the magnetic stripe; and innovative technologies.

Card Not Present and Mobile Security

The *Card Not Present and Mobile Security* working group will develop methods to enhance payment security in the mobile or card-not-present environments. E-commerce and other technology innovations increase the frequency of transactions that happen without the card present. We must understand that our obligation to protect consumer data must factor into this new reality and identify ways to bolster our defenses.

Similar to the previous working group, the specifics are being developed but elements under consideration include: end-to-end data encryption; tokenization; customer identification improvements; and the ability to leverage new, more secure next generation top level domain environments to be launched by the financial services industry.

Cybersecurity & Data Breach Notification

The Cybersecurity and Data Breach Notification working group will identify the appropriate legislative policy to ensure the private sector takes actions necessary to notify and protect consumers if a breach occurs.

The group is considering whether there should be a federal standard for breach notification, steps to better coordinate with law enforcement agencies, as well as additional tools legislators could authorize to enhance cyber security and better protect consumers.

While we will continue to pursue industry solutions to better protect consumers, there is an important need for Congressional action.

Congressional Action

The question before the Committee today is what government can and should do to bolster the private sector and increase our ability to protect consumers. As a partnership, we are considering that very same question.

Senators Carper and Blunt have introduced S. 1927, the "Data Security Act of 2014." Their legislation preempts state law on issues related to data security, investigation, and notice. The legislation establishes a notification standard that is based on "substantial harm or inconvenience." And, financial institutions that comply with Graham-Leach-Bliley Act standards would be deemed in compliance on notification requirements.

I cannot speak on behalf of the partnership because we are still developing our views, but I can say that the Financial Services Roundtable appreciates the legislation and looks forward to working with the Senators and this Committee to achieve its objectives.

But more important than breach notification requirements are the efforts to prevent data breaches in the first place. To that end, FSR and many others have focused on effective cyber threat information sharing. Institutions must have the necessary liability protections to share threat information with private partners and the government. Further, those liability protections should extend to good faith actions taken to defend data, the financial system, and consumers.

We cannot overstate the importance to our industries and our customers of passing this legislation. Having the freedom to share information will give us an improved ability to stop attacks in real time and prevent attacks from occurring in the first place. While we understand and respect privacy concerns, the benefits from this legislation far outweigh potential downsides. FSR supported the *Cyber Intelligence Sharing and Protection Act of 2013*, commonly known as CISPA passed by the House. We understand that the Senate Intelligence Committee is actively working on cyber threat information legislation and we strongly and urgently encourage those efforts.

While the financial services sector continues to improve information sharing communications, the progress will likely remain inadequate without congressional actions to enhance, facilitate, and protect threat information sharing across sectors and with government. Information sharing

legislation would further strengthen the ability of the private sector and the federal government to work together to develop a more effective information sharing framework.

Conclusion

Rather than retreating to our respective silos, the retail and financial services sectors have decided to work together to benefit our customers and the economy. Increased cyber security may lead to some short-term cost increases and inconveniences, but it is an investment well worth making. We believe the partnership between the financial services and retail industries will be very helpful. We will keep you informed of our efforts and appreciate the Congress' level-headed examination of cyber threats to our economy. We also hope you will pass the legislation we referenced here today. It is overdue and urgently needed.

Thank you for the opportunity to appear before this Committee. I look forward to continuing to work with you to address cyber-security, data breaches and many other issues. I would be happy to address any questions the Committee may have.