TESTIMONY OF

TOM LITCHFORD

VICE PRESIDENT OF RETAIL TECHNOLOGIES,
NATIONAL RETAIL FEDERATION

BEFORE THE HOUSE HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION, AND SECURITY
TECHNOLOGIES

HEARING ON

"Protecting Your Personal Data: How Law Enforcement Works
With the Private Sector to Prevent Cybercrime"

APRIL 16, 2014

National Retail Federation
1101 New York Avenue, NW
Suite 1200
Washington, DC 20005
(202) 626-8126
www.nrf.com

Chairman Meehan, Ranking Member Clarke, and members of the Subcommittee, thank you for giving me this opportunity to provide you with my thoughts on safeguarding consumer information from cyber-attacks. My name is Tom Litchford, and I am Vice President of Retail Technologies at the National Retail Federation (NRF). In my role at the NRF, I manage the CIO Council, the IT Security Council, and the Association for Retail Technology Standards.

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing $2.5 trillion to annual GDP, retail is a daily barometer for the nation's economy.

With respect to consumer data breaches I'd first like to comment on an often forgotten fact – that these incidents have been perpetrated by criminals – and often very sophisticated criminals – that are breaking the law. The targeted retailers are victims in these situations – victims that care very deeply about maintaining the confidentiality of their customer information because if they lose that data, they lose their customers' trust, and they lose business.

Accordingly, retailers make significant investments every year in order to protect this data. Collectively, retailers spend billions of dollars annually to safeguard data and fight fraud, as well as hundreds of millions annually on PCI compliance. And yet, breaches still occur. And not just in the retail industry. You may be surprised to learn that in 2013 more breaches happened at financial institutions than at retail stores and websites. Manufacturing, transportation and utility companies, and even professional services firms were targeted. No industry is immune.

In retail breaches, the bad actors are primarily after payment data – i.e., credit or debit card numbers – and they particularly like to target US cards. Why? Because of the volume of credit and debit card numbers, and the fact that merchants must accept from customers fifty-year old payment card technology – a magnetic stripe and a signature are all that is needed to "authenticate" the customer and receive payment authorization. The bottom line is that signature and mag-stripe based cards are inherently fraud-prone products. Unfortunately, retailers and our customers are largely at the mercy of the dominant credit card companies when it comes to reducing card fraud.

So, how can we move forward? What types of solutions would reduce or eliminate the crimes of data theft and fraud?

<u>The Way Forward to Protect the Retail Industry</u>

One solution would be to replace signature authentication with an encrypted Personal Identification Number (PIN). This would greatly reduce the utility of counterfeited cards and go a long way toward reducing fraud.

Another solution that is currently receiving some attention would be to add a computer chip to the PIN and transition to the more secure "Chip and PIN" payment card technology. This technology employs a small computer chip to validate the card to the bank (i.e., confirm that it is not a counterfeit) at the Point-of-Sale (POS) terminal, in addition to requiring the cardholder to enter a PIN to prove he is the person authorized to use the bank-issued card. Chip and PIN technology dramatically reduces the value of any stolen "breached" data for in-store purchases because the payment card data is essentially rendered worthless to criminals. In addition, the PIN helps ensure that a customer and a merchant won't be defrauded even if someone steals the customer's card. This combination serves as a deterrent to breaches. The failure of U.S. card networks and banks to adopt such a system in the U.S. is one reason why cyber-attacks on brick-and-mortar retailers have increased domestically even as they have dropped overseas where the majority of the countries have adopted Chip and PIN payment cards.

Despite the technology's potential benefits, the Chip and PIN technology that is currently widely deployed in Europe and other developed countries, sometimes called "EMV technology," would not provide the same level of protection in the U.S. because, as mandated by the card brands for the U.S. market, it does not require the use of a PIN. EMV – an acronym for Europay, Mastercard and Visa – is a proprietary technology controlled by the major card brands. Further, EMV, while not necessarily violating the Durbin Amendment, currently violates the spirit of that amendment by potentially stifling the competition in the debit routing market.

No technology (and especially not EMV), is a panacea, and there is no "silver bullet" to preventing cybercrime. EMV, in particular, would take years to realize the benefit in fraud reduction. As a result, our members are exploring other means of securing data, such as encryption and tokenization. Equally important, in addition to technological changes, our members are developing measures, such as establishing information sharing mechanisms, to address the advanced threats of the evolving cybercrime landscape.

The Value of Information Sharing

One critical aspect of next generation information security is the ability to share and receive actionable threat intelligence in a timely manner. Information sharing allows companies to better detect and defend against sophisticated cyber-attacks and data security breaches. By working together and with government to disseminate and receive cyber threat information, companies can learn where to look for signs of an attack and how to alter their security systems to "plug holes" and block attempted intrusions carried out using techniques that were effective in earlier attacks.

Importantly, third parties often possess information that can help us mitigate the risks of an attack. As the United States Secret Service (USSS) recently acknowledged in testimony before the Senate, "one of the most poorly understood facts regarding data breaches is that it is rarely the victim company that first discovers the criminal's unauthorized access to their network; rather it is law enforcement, financial institutions,

or other third parties that identify and notify the likely victim company of the data breach by identifying the common point of origin of the sensitive data being trafficked in cybercrime marketplaces."[1] Victims of cybercrime can then begin to extricate fraudsters from their system and prevent further data loss when they know that an attack has taken place. Creating structures where information regarding critical threats – and certainly actual breaches – is shared swiftly can be critical in preventing and minimizing losses from data breaches.

The retail industry is in a particularly good position to both benefit from and bring value to information sharing with outside organizations and entities. Indeed, the history of data breaches affecting the retail industry indicates a pattern of increasingly sophisticated cyber-attacks using similar tactics, techniques and protocols (TTPs). During the recent spate of data breaches targeting the retail industry, the sector learned the value of such information sharing by receiving various reports and alerts from the USSS and FBI, as well as other federal agencies (e.g., US-CERT and NCCIC) that highlighted cutting-edge TTPs. The retail industry also received valuable information from security research companies; for example, the iSightPartners report, which was disseminated through the National Cybersecurity and Communications Integration Center (NCCIC) in the wake of the Target breach, was of such particular value that NRF subsequently held a webinar for its membership where an iSightPartners' representative presented on the report's findings. In addition, in January 2014, the FBI shared a confidential report with the retail industry titled "Recent Cyber Intrusion Events Directed Toward Retail Firms" that was designed to warn the industry regarding "memory-parsing" malware that can infect POS systems. While the warnings in the report – and the findings of the iSightReport – were useful to the retail sector, NRF realized that its members would have derived significant additional benefits had they been shared sooner. It would have been more helpful had an established, trusted entity representing the retail sector existed , at the time, to receive such information in real-time and disseminate it to credentialed retail business security officers.

One effective mechanism for sharing information, with a proven track record, is sector-specific Information Sharing and Analysis Centers (ISACs). In 2006, the Department of Homeland Security recommended that the nation's critical infrastructure sectors develop ISACs to more effectively share threat intelligence. Today, the National Council of ISACs has 15 member ISACs, including 13 representing or related to critical infrastructure sectors. While the retail industry is not critical infrastructure, NRF believes that the sector could benefit from taking a similar approach to information sharing. ISACs provide a trusted source and repository for critical threat information, whether provided by outside organizations or internal members.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) has been a leading example of a model that has assisted one sector in preparing for and defending

[1] Testimony of Criminal Investigative Division Deputy Special Agent in Charge William Noonan, available at: https://www.dhs.gov/news/2014/02/04/written-testimony-us-secret-service-senate-committee-judiciary-hearing-titled-

against cybercrime. The FS-ISAC established various forums and tools to encourage and support information sharing among its members. Those include e-mail alerts that provide timely and actionable cyber threat intelligence, bi-weekly threat information sharing calls with security or risk management experts, as well as emergency conference calls to share particularly urgent threat intelligence. The FS-ISAC also conducts online webinar presentations for its members so they can share threat information and best practices. Using those tools, the financial services industry as a whole can remain aware of the most up-to-date attack prevention measures. As outlined in the next sections, NRF has already taken steps to create, or is in the planning stages of developing, similar mechanisms to encourage information sharing within the retail industry. The ultimate goal of these endeavors is to establish a robust ISAC equivalent for the retail industry. (Retail ISAC)

Steps NRF Has Taken to Create a Trusted Information Sharing Platform

NRF already brings together senior business, technology, and loss-prevention leaders through its Chief Information Officer (CIO) Council. One subcommittee within this Council, the IT Security Council, connects information security professionals and focuses on, among other goals, promoting information sharing within the retail sector. NRF is currently using its authenticated IT Security Council email distribution list (and expanding it to also include business leaders from the CIO Council) to push out actionable threat intelligence to the retail industry. While this list currently includes only NRF members, the intention is to broaden the list, and forthcoming Retail ISAC membership, to non-NRF members as well (meaning all retailers).

Another step NRF has taken on the road to creating a Retail ISAC is to collaborate with, and learn from, the FS-ISAC. NRF has held several meetings with the FS-ISAC regarding its structure, communication methods, and policies. These meetings have allowed NRF to gain insight into how to operate an effective ISAC and avoid some of the growing pains that come with the creation of any new entity. As a result of these initial discussions, the FS-ISAC and NRF have taken steps to establish a mechanism to push out relevant critical threat information from the FS-ISAC to NRF for further distribution to its authenticated IT Security Council members. The practical experience of receiving information through an ISAC will allow NRF to better understand how information is shared in an ISAC, and what filtering is necessary to ensure that useful information is reaching the right parties.

NRF is also establishing relationships with key government agencies. The government collects valuable information regarding security incidents through its cybercrime investigations and broad information sharing activities. NRF has held meetings with the United States Secret Service to discuss the methods the agency currently uses to distribute critical threat information, and how the Retail ISAC could become a valued partner. Establishing a Retail ISAC will offer a quicker avenue for the USSS (and other law enforcement agencies) to share valuable information with the retail industry.

NRF has also met recently with the National Cybersecurity and Communications Integration Center to discuss how the Retail ISAC could receive actionable intelligence

for its members as quickly as possible. The NCCIC is a central communications point for critical infrastructure entities, various government agencies and international investigators where cybersecurity information is sent, analyzed and shared with relevant parties in real time. NCCIC consists of four branches, including the U.S. Computer Emergency Readiness Team (US-CERT). These connections with the USSS and NCCIC are helping to establish an information sharing bridge to the retail industry even as the Retail ISAC is under development.

Working with trusted advisors, NRF is currently in the planning stages with respect to a final step in the development of the Retail ISAC: the establishment of the technological and operational infrastructure to support a secure portal through which members can share information. NRF's goal is to allow credentialed members to share information of varying levels of sensitivity anonymously, thus allowing the Retail ISAC to act as a repository of critical threat, vulnerability and incident information that is sourced from various members and outside organizations, and to facilitate peer-to-peer collaboration with the sharing of risk mitigation best practices and cybersecurity research papers. As this final step is resource-intensive and requires the active participation of its membership, NRF anticipates that it may take several months before the Retail ISAC is fully operational. In the meantime, NRF has, and will continue to, provide mechanisms and tools for information sharing among the retail industry, as outlined above.

As a final note on information sharing, NRF and its membership recognize that full, robust information sharing is sometimes hampered by legal restrictions. Accordingly, NRF supports the passage by Congress of the bipartisan "Cyber Intelligence Sharing and Protection Act" (H.R. 624) so that the commercial sector can lawfully share information about cyber-threats in real time, thereby enabling companies to defend their own networks as quickly as possible from cyber-attacks that are detected by other businesses.

Conclusion

In closing, there are three important policies that NRF supports.

First, the members of NRF support replacing today's fraud-prone mag-stripe and signature cards with cards using PINs or open-standard "Chip and PIN" technology. NRF also supports efforts to develop and deploy end-to-end encryption or tokenization, but is opposed to the adoption of "EMV" technology as mandated for the U.S. market, as it presently would not require PIN-authentication of card-holders and rely instead on simply a signature to authenticate the consumer.

Second, NRF supports information-sharing within its membership and the retail industry about cyber threats and has already taken several steps to create a Retail ISAC, and continues to actively engage in making that goal a reality. A retail-focused ISAC will allow the industry as a whole to benefit from the information sharing that is so critical to effectively combat today's evolving cyber-threat.

Third, we support passage by Congress of the bipartisan "Cyber Intelligence Sharing and Protection Act" (H.R. 624) legislation that will facilitate the sharing of cyber-threat information in real time, thereby enabling companies to better defend their own networks based on critical information about attacks on other businesses.

Thank you for your time today. I'd welcome your questions.