TESTIMONY OF SANDRA L. KENNEDY

PRESIDENT,
RETAIL INDUSTRY LEADERS ASSOCIATION

BEFORE THE

SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS COMMITEE

HEARING ON

"DATA BREACH ON THE RISE: PROTECTING PERSONAL INFORMATION FROM HARM"

APRIL 2, 2014

Chairman Carper, Ranking Member Coburn and members of the Committee, my name is Sandra Kennedy and I am the President of the Retail Industry Leaders Association (RILA). Thank you for the opportunity to testify today about the cybersecurity threats we collectively face and the steps that the retail industry is taking to address them and protect consumers. I am particularly pleased to be testifying alongside Governor Tim Pawlenty, CEO of the Financial Services Roundtable, to share details about a unique inter-industry partnership aimed at strengthening protections for consumers.

RILA is the trade association of the world's largest and most innovative retail companies. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together are responsible for more than $1.5 trillion in annual sales, millions of American jobs and more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

The threat of cyber attacks is understood now to be all too common. While retailers place extremely high priority on data security, cyber-criminals are persistent and their methods of attack are increasingly sophisticated. As we have seen, no organization, be it business, education or government, is immune from attacks. Recent reports that federal agents in the last year alone notified more than 3,000 businesses of breaches to their systems offer a sense of the scale of the threat and the persistence of the criminals.

I. Defending Against Cyber Attacks

Retailers take the threat of cyber attacks very seriously, investing tremendous resources in talent and technology to defend against them. But as experts testifying before this Committee have noted, while security measures help thwart attacks, no system is invulnerable. Retailers understand that defense against cyber attacks must be an ongoing effort, evolving to address the changing nature of the threat. To that end, in January, with the support of our Board of Directors, RILA launched a comprehensive Cybersecurity and Data Privacy Initiative. The initiative is designed to enhance the industry's existing cybersecurity and privacy efforts, inform the public dialogue, and build and maintain consumer trust.

RILA's initiative addresses three areas: overall Cybersercurity; enhanced Payment Systems Security; and Consumer Privacy. I will describe each in turn.

A. Cybersecurity:

Formation of a Retail Cybersecurity Leaders Council – Retailers rebuff cyber attacks every day and the resulting lessons learned can, if shared, strengthen protections across the entire industry. The Retail Cybersecurity Leaders Council, which is made up of senior retail executives responsible for cybersecurity, is working to improve industry-wide cybersecurity by sharing threat information and discussing effective security solutions in a trusted forum.

Federal Data Breach Notification Legislation – RILA has engaged with lawmakers to promote federal data security breach notification legislation that sets a national baseline.

Federal Cybersecurity Legislation – RILA has committed to engage with policymakers to help develop federal cybersecurity legislation focused on enabling measures widely viewed as being effective to strengthen cybersecurity such as appropriate information-sharing and R&D investments.

B. Improved Payments Security:

Eliminate the Mag-Stripe: The existing magnetic stripe technology used on credit and debit cards issued in the United States is antiquated and vulnerable. RILA is advocating that it be phased out in favor of more secure technology widely used in other parts of the world.

Universal PIN Security and Chip-based Smart Card Technology - RILA will continue to press the card networks and the issuing banks to migrate to universal PIN security and chip-based smart card technology. In the event of a successful cybersecurity breach, the dynamic security features of such technology renders stolen card data largely useless.

System-Wide Collaboration - Enhanced card security is an important first step, but innovation in the payments security must outpace criminal threats. Therefore, RILA has committed to forge a partnership with the other members of the payments ecosystem to collaborate on long-term, comprehensive approaches to address evolving threats.

C. Consumer Privacy:

RILA's cybersecurity and payments security efforts will go a long way to help address consumer privacy expectations, as consumers want and expect data about them to which retailers have access to be protected. Consumers also welcome tailored services, yet may have questions about the data practices required to provide them. RILA has convened a forum in which retailers can develop and share data and privacy insights and best practices, and where useful we will help to shape and then promote data practices that are consistent with RILA's privacy principles.

In the months since its launch, the initiative has made progress on multiple fronts.

The Retail Cybersecurity Leaders Council (Council) has begun work to establish a mechanism for improved industry-wide threat information sharing. A recent survey of the group found that a majority of RILA members already participated in informal or non-retail specific threat information sharing, but that

expanding such efforts to include engagement with other partners and government would bolster efforts to defend against the growing threat. This group has already made considerable progress toward establishing a trusted forum through which threat information can be better shared among trusted parties.

Specifically, through the Council, RILA recently formed a partnership with the National Cyber-Forensics and Training Alliance (NCFTA), a respected non-profit organization specializing in establishing public-private partnerships. The NCFTA partnership will provide retailers with an established and trusted forum where retailers can collaborate with a diverse set of businesses and government agencies on effective solutions to combat cyber-criminals.

Just last week, the Council convened over twenty-five retail executives from some of America's largest retailers for a two-day conference at the NCFTA facilities in Pittsburgh, PA. The group explored various information-sharing models and governance structures, and met with experts from government, law enforcement, academia, and solution providers to gain further insight on the cyber threat landscape and leading practices in cybersecurity. This meeting was very productive and there was broad consensus in the group in support of continued collaboration and information sharing.

.

II. Data Breach Notification

When attacks are successful and compromise customer data, retailers believe that their customers have the right to be notified as promptly as possible. Retailers also believe that they have an obligation to provide customers whose personal information has been compromised with information that is as accurate and actionable as possible so that they can take steps to protect themselves. In order to notify customers as quickly as possible, in RILA's experience retailers typically conduct their response in parallel tracks – while one group investigates the attack to determine if there was unauthorized access to or acquisition of personal information, a second group begins preparing to distribute notifications as necessary to affected customers.

Where feasible, retailers provide direct notification, such as written notification by mail, email or phone. Merchants also may alert customers through alternative means such as website postings or the media.

To improve upon current processes, RILA supports federal data breach notification legislation that is practical, proportional and sets a single national standard that replaces the patchwork of state laws in place today. A federal standard will help ensure that customers receive timely and accurate information following a breach. Any legislation considered by Congress should include three essential provisions. First, legislation should include strong state preemption language that would create a single national standard. Second, legislation should consider the practical realties following a breach. Specifically, adequate time must be allowed prior to a mandated notification in order to allow organizations to secure the breached environment, conduct a thorough forensics investigation and then, based off this assessment, determine who may have been affected by the cyber attack and what information was compromised. Furthermore, reasonable delays in notification should be allowed if requested by law enforcement for investigative purposes or national security reasons. Third, notification requirements should be linked to risk of harm, for example considering whether or not the compromised information is in a form usable to commit financial fraud or identify theft.

III. Legislative Proposals

As you know, there have been multiple bills introduced in both the Senate and House of Representatives in relation to data breach notification, including one by Chairman Carper. While RILA has yet to take a position on any of these bills, we believe that it is imperative that strong state preemption be a part of any legislation. As the bills move through the legislative process, RILA looks forward to working with Congress on enacting legislation that provides customers with concise, accurate and timely notification.

IV. Partnership between Merchants and Financial Services

While there is much that retailers can undertake as an industry, retailers recognize that much more can be done by collaborating with other stakeholders as well. Cyber criminals who attack retailers do so in hopes of accessing sensitive consumer financial information, specifically credit and debit card information. Retailers believe that a strong defense against cyber attacks requires not only that retailers stay ahead of the threats they face, but also that payments technology and process advance such that any stolen data cannot be used to counterfeit cards and commit fraud. For example, retailers believe that enhanced technology widely available elsewhere in the world known as Chip and PIN would render stolen data largely valueless to cyber criminals.

The interconnectedness of merchant and financial services industries, and the common obligation to protect our shared customers, is such that collaboration among the two industries is essential. To that end, in February, RILA joined with the Financial Services Roundtable and 16 other associations representing merchants and financial institutions of all types and sizes to establish Merchant – Financial Services Cybersecurity Partnership, a group that is dedicated to strengthening overall security across the payments ecosystem and bolstering consumer confidence in the payments system.

The historical tension between these two industries is well chronicled. And while we expect that there will continue to be issues on which we disagree, the common threat that we face is such that we have an obligation to consumers to find areas where we can work together. Thus far, we are encouraged by the level of participation from both industries.

Since its formation, the partnership has moved quickly to establish objectives and a process through which to achieve them. As such, the partnership has established five working groups, each made up of experts from participating associations' member companies. Each working group will have a focus area on which members will work to advance a consensus opinion that improves overall security.

The working group areas of focus are:

1. Threat Information Sharing
2. Cybersecurity Risk Mitigation
3. Advanced Card-Present Security Technology
4. Card-Not-Present and Mobile Security
5. Cybersecurity and Data Breach Notification

Given the complexity of the issues under consideration, participating associations have worked to select the appropriate subject matter experts to represent the interests of their membership. Nominations have

been received, groups have been populated with members, and the first meetings of the working groups will begin next week.

The tasks before these working groups are significant, but we believe they are achievable and we are committed to achieving significant progress by the end of 2014.

In closing, we believe that in working together with public and private sector stakeholders, our ability to develop innovative solutions and anticipate threats will grow, enhancing our collective security and giving our customers the service and peace of mind they deserve. I appreciate the opportunity to testify before you today and I look forward to your questions.