RETAIL INDUSTRY LEADERS ASSOCIATION
Educate.Collaborate.Advocate.

1700 N. Moore Street, Suite 2250, Arlington, VA 22209
Phone: (703) 841-2300 Fax: (703) 841-1184
Email: info@rila.org Web: www.rila.org

TESTIMONY OF

**BRIAN A. DODGE, EXECUTIVE VICE PRESIDENT,
COMMUNICATIONS AND STRATEGIC INITIATIVES**

RETAIL INDUSTRY LEADERS ASSOCIATION

BEFORE THE

**HOUSE ENERGY AND COMMERCE COMMITTEE
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE**

HEARING ON

"WHAT ARE THE ELEMENTS OF SOUND DATA BREACH LEGISLATION?"

JANUARY 27, 2015

Chairman Burgess, Ranking Member Schakowsky and Members of the Committee, my name is Brian Dodge and I am the Executive Vice President of Communications and Strategic Initiatives at the Retail Industry Leaders Association (RILA). Thank you for the opportunity to testify today about data breach legislation and the steps that the retail industry is taking to address this important issue as well as our broader efforts to guard against cyber-attacks and protect consumers. Retailers greatly appreciate the Committee's leadership in seeking to find a sensible path to federal data breach legislation.

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.

Retailers embrace innovative technology to provide American consumers with unparalleled services and products online, through mobile applications, and in our stores. While technology presents great opportunity, nation states, criminal organizations, and other bad actors also are using it to attack businesses, institutions, and governments. As we have seen, no organization is immune from attacks and no security system is invulnerable. Retailers understand that defense against cyber-attacks must be an ongoing effort, evolving to address the changing nature of the threat. RILA is committed to working with Congress to give government and retailers the tools necessary to thwart this unprecedented attack on the United States (US) economy and bring the fight to cybercriminals around the globe.

Key Cybersecurity Issues for Retailers

As leaders in the retail community, we are taking new and significant steps to enhance cybersecurity throughout the industry. To that end, RILA formed the Retail Cyber Intelligence Sharing Center (R-CISC) in 2014 in partnership with America's most recognized retailers. The Center has opened a steady flow of information sharing between retailers, law enforcement and other relevant stakeholders. These efforts already have helped prevent data breaches, protected millions of American customers and saved millions of dollars. The R-CISC is open to all retailers regardless of their membership in RILA.

For years, RILA members have been developing and deploying new technologies to achieve pioneering levels of security and service. The cyber-attacks that our industry faces change every day and our members are building layered and resilient systems to meet these threats. Key to this effort is the ability to design systems to meet actual threats rather than potentially outdated cybersecurity standards that may be enshrined in law. That is why development of any technical cybersecurity standards beyond a mandate for reasonable security must be voluntary and industry-led such as the standards embodied in the National Institute of Standards and Technology Cybersecurity Framework.

One area of security that needs immediate attention is payment card technology. RILA members have long supported the adoption of stronger debit and credit card security protections. The woefully outdated magnetic stripe technology used on cards today is the chief vulnerability in the payments ecosystem. This 1960s era technology allows cyber criminals to create counterfeit cards and commit fraud with ease. Retailers continue to press banks and card networks to provide US consumers with the same Chip and PIN technology that has proven to dramatically reduce fraud when it has been deployed elsewhere around the world. According to the Federal Reserve, PINs on debit cards make them 700 percent more secure than transactions authorized by signature.[1]

Increasing cyber threat information sharing also is vital to defeating sophisticated and coordinated cyber actors. RILA strongly supports cybersecurity information sharing legislation that provides liability protections for participating organizations. Legislation also should increase funding for government sponsored research into next generation security controls and enhance law enforcement capabilities to investigate and prosecute criminals internationally. The cyber-attacks faced by every sector of our economy constitute a grave national security threat that should be addressed from all angles.

When attacks on consumer information are successful and will cause economic harm, 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 with information that is as accurate and actionable as possible so that they can take steps to protect themselves. To that end, RILA supports federal data breach notification legislation that is practical, proportional and sets a single national standard that replaces the often incongruous and confusing patchwork of state laws in place today. A single, clear, preemptive federal standard will help ensure that customers

[1] Federal Reserve, "2011 Interchange Fee Revenue, Covers Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions," (March 5, 2013).

receive timely and accurate information following a breach. To place in context the need for preemptive federal data breach legislation, we provide below a brief overview of the significant data security and breach notification laws with which retailers currently comply.

Existing Data Security and Breach Notification Laws

Forty-seven states, the District of Columbia (DC), Guam, Puerto Rico and the US Virgin Islands have adopted data breach notification laws. While there are many variations across these laws, as a general matter, state data breach notification laws require notification to individuals, and under some circumstances, state law enforcement, regulators, the media, or consumer reporting agencies when there is a reasonable belief of unauthorized acquisition of or access to data that compromises the security, confidentiality or integrity of an individual's covered personal information. The majority of jurisdictions include some type of risk of harm threshold that mitigates the risk of over-notification to consumers of breach incidents. Retailers operating in each of the 51 jurisdictions, must reconcile different notice time requirements, disparate requirements regarding the content of the notice, as well as differing rules to notify the jurisdictions themselves among many other requirements. For companies operating across many jurisdictions, this fact dependent analysis must occur simultaneously, rapidly, and accurately. Retailers face a significant regulatory burden to comply with the vast number and variety of these breach notice laws.

In addition to 47 state data breach notice laws and the laws in DC and the US territories, retailers are subject to robust data security regulatory regimes relating to protections for sensitive personal information. At the federal level, the Federal Trade Commission (FTC) is the primary regulator of data security for most businesses across a wide array of industry sectors, including the retail sector. Under Section 5 of the FTC Act, the FTC has authority broadly to bring enforcement actions against companies that engage in "unfair or deceptive acts or practices in or affecting commerce."[2] Although the FTC has not promulgated data security rules, its robust enforcement activity has collectively created a "common law" of consent decrees that tend to signal what is expected from businesses regarding the collection, use, and protection of personal information. The consent decrees usually involve non-monetary remedies requiring the implementation of comprehensive company privacy or data security programs with biennial audits for up to 20 years. The FTC can impose penalties of up to $16,000 per violation for violations of a consent decree.

The FTC uses both its authority to prevent consumer deception and unfairness to enforce data security standards.[3] Pursuant to its authority to prevent deceptive acts or practices, the FTC can and does bring enforcement actions against companies that have failed to comply with their data security representations and statements in their public-facing privacy policies or other disclosures. Pursuant to its authority to prevent unfair acts and practices, the FTC has pursued companies that have failed to deploy reasonable and appropriate security measures to protect the sensitive personal information they possess or handle (e.g., Social Security numbers, financial

[2] 15 U.S.C. § 45(a)(1).

[3] FTC, US Senate Banking Committee Hearing on Safeguarding Consumers' Financial Data (2014), *available at* http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=e6f6163c-ae31-4091-8e7c-c10e1eebbe84.

account or payment card information, and other information that can lead to fraud or identity theft) using its Section 5 enforcement power.

Since 2001, the FTC has settled at least fifty cases against businesses that it charged with failing to provide reasonable data security practices. The FTC conducts enforcement investigations with a focus on reasonableness, and has stated that "a company's data practices must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[4] Over time, the FTC's enforcement actions and other guidance materials,[5] have created a robust set of data security expectations applicable to businesses under its jurisdiction. The FTC expects that companies implement a comprehensive information security program containing safeguards to address administrative, physical and technical risks to personal information.

Inadequate data security measures for personal information also can lead to violations of state laws. Many state laws require businesses to do some combination of the following: (1) comply with data security rules for personal information; (2) maintain the confidentiality of Social Security numbers; and (3) securely dispose of personal data. In addition to express statutory provisions relating to data security, many states have so-called "Little FTC Acts" that also can be used by state Attorneys General to enforce against what the Attorney General deems to be unreasonable data security practices.

While retailers diligently comply with this patchwork of state data breach notice and data security laws as well as federal data security requirements, a carefully crafted federal data breach law has the potential to clear up regulatory confusion, remove conflicting rules, and better protect and notify consumers.

RILA Supports Sound Data Breach Legislation

RILA supports data breach legislation that includes a number of key elements that will protect consumers and allow retailers to continue to grow and innovate in our global and interconnected economy. The first goal of a successful federal statute should be to better protect customers and reduce the state-level burden on interstate commerce. To address this goal, retailers support strong preemption of state data breach notice and data security laws. Nobody benefits from the confusing variety of data breach notification laws in forty-seven states plus the District of Columbia, Guam, Puerto Rico and the US Virgin Islands. Strong preemption is necessary to ensure that a federal law is not the fifty-second data breach law with which retailers must comply. Similarly, a federal law should not include regulatory authority to allow the FTC to change notification rules, which will undercut the goal of creating a single and predictable national breach notification standard.

---

[4] FTC, US Senate Banking Committee Hearing on Safeguarding Consumers' Financial Data, 4 (2014), *available at* http://www.banking.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=e6f6163c-ae31-4091-8e7c-c10e1eebbe84.

[5] *See* FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2011), *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

The second goal of data breach legislation should be to provide timely and accurate notice to consumers. Retailers support a reasonable timeframe to provide notice. The timeframe should be triggered by the confirmation of a breach and bound by the time it takes to investigate and verify facts, as fact-based notification provides customers with proper information through which to determine what action to take. Importantly, priority should be given to law enforcement seeking to apprehend cybercriminals. Notification requirements should therefore be delayed if requested by law enforcement. Moreover, requirements as to how notice must be given should be flexible and include alternatives to allow a business to reasonably reach customers when a business does not possess contact information at the time of the breach.

The third goal of data breach legislation should be targeted and clear notice when customers face real harm. Retailers support providing reasonable notice to consumers. Notice should be provided when there is a reasonable belief that a breach has or will result in identity theft, economic loss, or harm. The majority of state laws recognize that linking notice to harm is vital to enabling customers to be vigilant and potentially take action to mitigate harm. Inundating customers with notice of every systems penetration would create a perverse outcome where customers will be less likely to pay attention to breach notices or less likely to discern between breaches that may impact them and those that have no customer impact.

The fourth goal of data breach legislation should be to require that notice be provided by the entity breached. The obligation to notify and publicly acknowledge a breach creates a clear incentive to enhance a company's data security. Directing all notice obligations to entities with first party relationships removes that important incentive. While the obligation should attach to the party breached, the law should provide flexibility for entities to contractually determine the notifying party.

The fifth goal of data breach legislation should be to avoid an overly broad scope. Retailers support a precise and targeted definition of personal information. It is important that notice and data protection occurs only when consumers face real peril from the exposure of sensitive data and need to be vigilant and potentially take action. An overly broad definition that includes harmless or publicly available data will both detract from the effectiveness of the notice (over-notifying) and chill the innovative use of data by the private sector. Differentiating between truly sensitive data requiring more restrictive security controls and harmless data that can be used more dynamically to create the next great product, service, or customer experience is vital to retailer innovation. Sweeping harmless data into the personal information definition undermines product development and the future economic growth of 21st century retailers. Also, an overbroad definition of personal information undermines a core goal of breach notice legislation, which is to provide carefully calibrated notice allowing consumers to prevent harm. Consumers that begin to ignore important communications are powerless to mitigate harm.

The sixth goal of data breach legislation should be to protect consumer data. Retailers support a carefully calibrated reasonable data security standard. If policymakers choose to address data security, the law must be carefully calibrated to recognize existing obligations and encourage companies to adhere to leading security practices. Legislating technology and prescribing technical standards will undermine cybersecurity innovation. The rapid pace of technological

change ensures the obsolescence of laws that are not technology neutral. Specific standards are best left to multi-stakeholder open standards setting organizations with the technical expertise, agility, and ability to move at Internet speed.

The final goal of data breach legislation should be to ensure fair, consistent, and equitable enforcement of a data breach law. Enforcement of the law should be consistently applied by the FTC based on cases of actual harm. Similarly, to the extent civil penalty authority is provided, this authority should be capped based on actual harm to consumers. Also, any legislation should deny a private right of action as it would undermine consistent enforcement.

We look forward to working with the Committee on specific language to address each of the above goals.

Retailers are Committed to Protecting Customer Data and Enhancing Consumer Trust

Retailers are committed to protecting our customers through investments in cybersecurity technology and personnel, increased cyber threat information sharing through a new law and the Retail Cyber Intelligence Center, and support for sound federal data breach legislation that is practical, proportional and sets a single national standard that replaces the patchwork of state laws in place today. We are engaging with policymakers and all stakeholders to advance each of these initiatives. I thank the Committee for considering the need for preemptive data breach legislation and look forward to answering your questions.