RETAIL INDUSTRY LEADERS ASSOCIATION

1700 North Moore Street
Suite 2250
Arlington, VA 22209

www.rila.org

March 14, 2019

Senator Mike Crapo
Chairman of the United States Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Senator Sherrod Brown
Ranking Member of the United States Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

The Retail Industry Leaders Association (RILA) welcomes the Senate Banking, Housing and Urban Affairs Committee's requests for comments on the collection, use and protection of sensitive information by financial regulators and private companies.

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 account for more than 1.5 trillion dollars in annual sales, millions of American jobs and more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

Data breach reform legislation has encountered a number of hurdles over the past decade. During the past several years, RILA has testified before the primary committees in the House of Representatives and has been working with peer trade associations to provide a roadmap that Members of Congress could utilize to avoid industry disagreements. RILA is encouraged by the Committee's desire to engage on these issues and we look forward to working together.

One of the key areas of contention between industries over the past several years has centered around a data security standard. RILA members support a carefully calibrated reasonable data security standard that focuses on size, cost, scope and complexity of a covered entity. Policymakers should recognize existing obligations and encourage companies to adhere to leading security practices and avoid legislating technology or prescribing technical standards that 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.

As retail and technology converge, maintaining customer trust is the bedrock of the retail business model. One-way retailers maintain trust is by making sure our partners care for our customers' data in the same manner we do. While retailers make every effort to hold our partners to account, we believe Congress can take a concrete step to make consumer protection the default. The Committee should require third parties

who hold consumer data to be held responsible and notify consumers if they have a breach. Enshrining this standard into law aligns all incentives to protect consumers.

Certain industries will say only the consumer facing company should notify the consumer and that antiquated state laws should stay in effect. This approach sacrifices consumer protection for expedience and profit and leaves consumers less secure. All companies who hold precious consumer data should be accountable to consumers. Equifax serves as one recent reminder of a non-consumer facing company holding extremely sensitive customer data with no responsibility to properly notify impacted consumers.

RILA believes that consumer facing companies can work together with third parties to communicate effectively to consumers. We also believe consumers are smart and can understand that companies partner with other companies to provide great services. Third parties provide important services to retailers and to the customers we serve. It is important as the Committee moves forward with potential breach legislation that they stand with consumers and specifically require all parties to be held to the same standard.

One of the core pillars in the breach debate has focused on providing timely and accurate notice to consumers in the wake of a breach. RILA supports 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 it does not possess contact information at the time of the breach.

As this discussion moves ahead, it is important to highlight some of our concerns on legislative language that focuses on "immediate notification." We are concerned this language could lead to confusion for the consumer because the proper investigation has not concluded, and therefore the scope of compromised data and impacted consumers is unknown. This will lead to inaccurate information being relayed to the public and further exasperation of an already difficult situation. In addition, companies should have reasonable time to address the practical realities of large-scale notification, i.e. establishing customer call centers, disseminating proper information to consumer facing employees, etc. The goal of notification should be to notify fast and correctly. RILA shares the goals for this language but urges caution. There is nothing more important to our members then the trust of their customers and RILA looks forward to working with the Committee to provide the right balance to guarantee the American consumer is notified in an accurate and expedited manner.

As the notification process is updated to reflect the changing economy, it is also imperative that all industries meet the same obligations to notify under this new structure. While RILA believes financial institutions notify if they are breached, the process behind this notification is opaque at best. This confusion can be easily ameliorated by including financial institutions under the new notification regime.

This will hold all industries to the same standard, and more importantly, will guarantee the American public will receive the same accurate and timely notification when a breach occurs from all business sectors.

Finally, one of the key provisions in the breach debate is on the creation of a federal statute that better protects customers and reduces the state-level burden on interstate commerce. To address this goal, RILA has long supported a strong preemption of state data breach notice and data security laws. Nobody benefits from the confusing variety of data breach notification laws in all fifty states plus the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands. Strong preemption is necessary to ensure that a federal law is not the fifty-forth data breach law with which retailers must comply.

In conclusion, RILA appreciates the Committee's efforts in navigating the myriad policy challenges centering around data breach legislation. While our comments focus on the key pillars of potential legislation, there are still other key topics that may impact this discussion including the provisions of a potential comprehensive federal privacy law. RILA looks forward to continuing our conversations with policymakers and all stakeholders to resolve our differences and enshrine federal data breach reform legislation into law.

Sincerely,

Austen Jensen
Senior Vice President, Government Affairs