Prepared Statement of Edith Ramirez
Senate Commerce Committee
March 26, 2014

Chairman Rockefeller, Ranking Member Thune, and members of the Committee, I appreciate the opportunity to present the Federal Trade Commission's testimony on data security.

Under your leadership, Chairman Rockefeller, this Committee has led critical efforts in Congress to protect consumers' privacy and data security. From the recent examination of the data broker industry and its impact on consumers to proposing data security requirements for industry, you and members of the Committee have sought to advance the same goals as the FTC. I want to thank you for your leadership.

As this Committee is well aware, consumers' data is at risk. Recent data breaches remind us that hackers seek to exploit vulnerabilities in order to access and misuse consumers' data in ways that can cause serious harm to consumers and businesses. These threats affect more than just payment card data. For example, breaches in recent years have also compromised Social Security numbers, account passwords, health data, and information about children. This occurs against the backdrop of identity theft, which has been the FTC's top consumer complaint for the last 14 years.

Today, I am here to reiterate the Commission's bipartisan call for the enactment of a strong federal data security and breach notification law. Never has the need for legislation been greater. With reports of data breaches on the rise, Congress must act.

The FTC supports federal legislation that would strengthen existing data security standards and require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Reasonable security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. And, when breaches do occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data.

Legislation should give the FTC authority to seek civil penalties where warranted to help ensure that FTC actions have an appropriate deterrent effect. In addition, enabling the FTC to bring cases against non-profits, such as universities and health systems – which have reported a substantial number of breaches – would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.

Finally, APA rulemaking authority, like that used in the CAN-SPAM Act, would allow the Commission to ensure that as technology changes and the risks from the use of certain types of information evolve, companies would be required to give adequate protection to such data.

For example, whereas a decade ago it would have been difficult and expensive for a company to track an individual's precise location, smartphones have made this information readily available. And, as the growing problem of child identity theft has brought to light in recent years, Social Security numbers alone can be combined with another person's information to steal an identity.

Using its existing authority, the FTC has devoted substantial resources to encourage companies to make data security a priority. The FTC has settled 50 cases against companies that we alleged put consumer data at risk. In all these cases, the touchstone of the Commission's approach has been reasonableness. A company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission has made clear that it does not require perfect security and that the fact that a breach occurred does not mean that a company has violated the law.

As the Commission's case against the retailer TJX illustrates, the Commission's data security cases have alleged failures to implement basic, fundamental safeguards. In 2007, TJX announced what was then one of the largest-known data breaches. According to the FTC's subsequent complaint against TJX, a hacker obtained information from tens of millions of credit and debit payment cards, as well as the personal information of approximately 455,000 consumers.

The FTC alleged that TJX engaged in a number of practices that, taken together, were unreasonable, such as allowing network administrators to use weak passwords; failing to limit wireless access to in-store networks; not using firewalls to isolate computers processing cardholder data from the Internet; and not having procedures to detect and prevent unauthorized access to its networks, such as procedures to update antivirus software.

In addition to our enforcement efforts, the Commission also undertakes policy initiatives to promote privacy and data security, such as workshops on mobile security issues and child and senior ID theft. And for those consumers who may have been affected by recent breaches, the FTC has posted information online about steps they should take to protect themselves. The FTC also provides guidance to businesses about reasonable security practices.

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumer data, and we look forward to continuing to work with the Committee and Congress on this critical issue.