Statement of Chairwoman Edith Ramirez
Committee on the Judiciary
U.S. Senate
Hearing on Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime
February 4, 2014

Chairman Leahy, Ranking Member Grassley, and members of the Committee, thank you for the opportunity to appear before you to discuss the Federal Trade Commission's data security enforcement program. I am pleased to be testifying with my colleagues from the Justice Department and the Secret Service.

We live in an increasingly connected world in which vast amounts of consumer data is collected. As recent breaches at Target and other retailers remind us, this data is susceptible to compromise by those who seek to exploit security vulnerabilities. This takes place against the background of the threat of identity theft, which has been the FTC's top consumer complaint for the last 13 years. According to estimates of the Bureau of Justice Statistics, in 2012 this crime affected a staggering seven percent of all people in the U.S. age 16 and older.

The Commission is here today to reiterate its bipartisan and unanimous call for federal data security legislation. Never has the need for such legislation been greater. With reports of data breaches on the rise, Congress needs to act. We support legislation that would strengthen existing data security standards and require companies, in appropriate circumstances, to notify consumers when there is a breach.

Legislation should give the FTC authority to seek civil penalties where warranted to help ensure that FTC actions have an appropriate deterrent effect. It should also provide rulemaking authority under the Administrative Procedure Act and jurisdiction over non-profits, which have been the source of a large number of breaches. Such provisions would create a strong consistent

standard and enable the FTC to protect consumers more effectively.

Using its existing authority, the FTC has devoted substantial resources to encourage companies to make data security a priority. The FTC has brought 50 civil actions against companies that we alleged put consumer data at risk. We have brought these cases under our authority to combat deceptive and unfair commercial practices as well as more targeted laws such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act.

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 the fact that a breach occurred does not mean that a company has violated the law.

Significantly, a number of FTC enforcement actions have involved large breaches of payment card information. For example, in 2008, the FTC settled allegations that security deficiencies of retailer TJX permitted hackers to obtain information about tens of millions of credit and debit cards. To resolve these allegations, TJX agreed to institute a comprehensive security program and to submit to a series of security audits. At the same time, the Justice Department successfully prosecuted a hacker behind the TJX and other breaches.

As the TJX case illustrates well, the FTC and criminal authorities share complementary goals. FTC actions help ensure, on the front end, that businesses do not put their customers' data at unnecessary risk, while criminal enforcers help ensure that cyber criminals are caught and punished. This dual approach to data security leverages government resources and best serves the interests of consumers, and, to that end, the FTC, the Justice Department and Secret Service

have worked together to coordinate our respective data security investigations.

In addition to the Commission's enforcement work, the FTC offers guidance to consumers and businesses. For those consumers affected by recent breaches, the FTC has posted information online about steps they should take to protect themselves. These materials are in addition to the large stable of other FTC resources we have for ID theft victims, including an ID theft hotline. We also engage in extensive policy initiatives on privacy and data security issues. For example, we have recently conducted workshops on mobile security and emerging forms of ID theft, such as child ID theft and senior ID theft.

In closing, I want to thank the Committee for holding this hearing and for the opportunity to provide the Commission's views. Data security is among the Commission's highest priorities, and we look forward to working with Congress on this critical issue.

Thank you.