Statement of Commissioner Edith Ramirez

Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
Washington, DC
June 15, 2011

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, I am Edith Ramirez, a Commissioner of the Federal Trade Commission. I appreciate the opportunity to present the Commission's testimony on data security. I want to thank you, Chairman Bono Mack, and the Committee for your leadership on this important issue.

Before I continue, I would like to note that my written testimony represents the views of the Federal Trade Commission, but my oral remarks and responses to questions are my own and may not reflect the views of the Commission as a whole or of other Commissioners.

As the nation's consumer protection agency, the FTC is committed to protecting consumer privacy and promoting data security in the private sector. If companies do not protect the personal information they collect and store, information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace. Although data security has recently been in the news, this is not a new priority for the FTC. To the contrary, for a decade, the FTC has undertaken substantial efforts to promote data security in the private sector through law enforcement, education, policy initiatives, and recommendations to Congress to enact legislation in this area.

Since 2001, the FTC has brought 34 cases charging that businesses failed to appropriately protect consumers' personal information. This includes a final settlement the Commission is announcing today against Ceridian Corporation, a large payroll processor. Ceridian's clients upload their employees' sensitive information—including Social Security Numbers and bank

account numbers—which is stored on Ceridian's network. The FTC's complaint charged that Ceridian did not maintain reasonable safeguards to protect this employee information; as a result, a hacker was able to gain access to it. The FTC's order requires Ceridian to implement a comprehensive data security program and obtain independent audits for 20 years.

The Commission also promotes better data security through consumer and business education. For example, on the consumer education front, we sponsor OnGuard Online, a website to educate consumers about basic computer security. Since its launch in 2005, there have been over 14 million unique visits to OnGuard Online and its Spanish-language counterpart Alerta en Línea. We also conduct outreach to businesses, especially small businesses, to provide practical advice about data security.

The Commission also engages in policy initiatives to promote data security. Last December, FTC staff issued a preliminary report proposing a new framework to improve consumer privacy and data protection. Among other things, the report advocates privacy by design, which includes several principles essential to data security: First, companies—no matter what their size—should employ reasonable physical, technical, and administrative safeguards to protect information about consumers. Second, companies should collect only that consumer information for which they have a legitimate business need. Third, businesses should retain data only as long as necessary to fulfill the business purpose for which it was collected and should promptly and securely dispose of data they no longer need.

As to legislation, the Commission generally supports federal legislation, similar to your draft proposal, that would (1) impose data security standards on companies and (2) require companies, in appropriate circumstances, to notify consumers when there is a security breach. Reasonable security practices are critical to preventing data breaches. And if a breach occurs,

prompt notification to consumers in appropriate circumstances can mitigate harm, such as identity theft. For example, in the case of a breach of Social Security numbers, notified consumers can request that fraud alerts be placed in their credit files, obtain copies of their credit reports, and scrutinize their monthly account statements. The Commission is pleased that your draft legislation includes civil penalty authority to deter violations, APA authority for rulemakings, and jurisdiction over non-profit entities for data security purposes. I would also like to note that both your draft legislation and the Commission staff's recent privacy report underscore the importance of data minimization to good data security.

The FTC looks forward to working with this Committee as it moves forward on the SAFE DATA Act. Thank you again for inviting me here today and for your leadership on these important issues. I will be pleased to answer your questions.