Statement of

IOANA RUSU
Policy counsel
Consumers Union

Before the

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Regarding

DATA SECURITY AND BREACH NOTIFICATION ACT OF 2010

September 22, 2010

Good afternoon Chairman Rockefeller, Ranking Member Hutchinson, and distinguished members of this Committee. My name is Ioana Rusu, policy counsel for Consumers Union, the non-profit publisher of *Consumer Reports*®. We appreciate the invitation by the Senate Committee on Commerce, Science, and Transportation to share our perspective on the Data Security and Breach Notification Act of 2010.

In January of this year, over 600,000 Citigroup customers were shocked to discover that that their Social Security numbers had been printed on the outside of envelopes containing annual tax statements. In July, a Lincoln National Life Insurance vendor printed a user name and password for agents and authorized brokers in a brochure, which was made readily available on the agent's public website. The login information allowed access to a website containing the medical records, Social Security numbers, addresses, policy numbers, and driver's license numbers of individuals seeking life insurance. And only last year, in one of the largest data security breaches recorded, malicious spyware compromised around 130 million credit card transactions processed by Heartland Payment Systems, a U.S. payments processing company.

These incidents are not unique or isolated. Almost every day, new data breach incidents lead to identity theft, lost revenue, and decreased consumer confidence in the way their personal information is handled in the marketplace. The incidents often occur through inadvertent disclosures, physical loss of stored paper or electronic records, data theft by company insiders, and data breach by third parties through hacking or malware. Sometimes, these incidents affect ten or twenty consumers. Other times, the private information of hundreds of millions of Americans is compromised.

The ubiquity of security breach incidents today renders the Data Security and Breach Notification Act of 2010 particularly timely and relevant. Consumers Union strongly supports the provisions of this bill. I would like to highlight a number of the bill's provisions, which we believe will best promote consumer data privacy.

First of all, we are pleased that the bill covers not only business entities, but also non-profit organizations, including private universities. Personal consumer data must be safeguarded by all those to whom it is entrusted, without regard to for-profit or non-profit status. Consumers face the same risks when their information is compromised, whether or

not the source of the compromise is a for-profit entity. As a result, we commend the bill's scope. This provision will provide more meaningful protection for consumer information.

In addition, we applaud the bill's notification provisions, which require covered entities to provide notice of security breach within 60 days of the breach. The sooner consumers are made aware of the breach, the quicker they can take remedial action such as closely monitoring their credit, checking their financial statements frequently, placing a federal fraud alert on their credit files, and placing a security freeze on their consumer credit files. The instances in which a covered entity may exceed the 60-day deadline are appropriate and narrowly tailored.

We also support the bill's requirements that covered entities provide at least two years of free credit reports or credit monitoring following a notice of breach. Consumers should not have to bear the costs of securing personal information when a data breach is caused by a company's inadequate data security practices.

The exemption in the bill, allowing covered entities to avoid the bill's requirements only as long as there is "no reasonable risk of identity theft, fraud, or other unlawful conduct," is also narrowly tailored.

However, we have some concern that, under this bill, all data breach incidents involving encrypted information, defined in the bill as information that has been rendered "unusable, unreadable, or indecipherable," would automatically be presumed to present "no reasonable risk of identity theft, fraud, or other unlawful conduct." While that may be true in most cases, data rendered "unusable or unreadable" can sometimes be reconstructed. We encourage the bill's sponsors to address this issue by directing the Federal Trade Commission to clearly identify which technologies do, indeed, render consumer data indecipherable and unusable.

We also support the bill's definition of "personally identifiable information," which includes not only an individual's name, in combination with one other listed data element, but also an individual's address or phone number, combined with one of the listed data elements. We believe including an individual's address and phone number is important due to the use of reverse search directories, which can reveal the person's name as long as an address or phone number is provided.

We are particularly pleased that the bill focuses on the activities of information brokers, defined as commercial entities whose business is to collect, assemble, or maintain personal information concerning individuals with the purpose of selling such information to unaffiliated third parties. We strongly support the provisions instructing information brokers to maximize the accuracy and accessibility of their records, as well as to provide consumers with a process to dispute information. In addition, the provisions requiring information brokers to submit their security policies to the FTC, as well to undergo potential FTC post-breach audits, will foster accountability and enforcement of this bill.

We strongly favor the provision that permits state Attorneys General and other officials or agencies of the State to bring enforcement actions against any entity that engages in conduct violating the bill. High-profile cases such as ChoicePoint and TJX have demonstrated that state attorneys general, in particular, have been at the forefront of notice of data breach issues, and have played an invaluable role in addressing identity theft and data breach. This bill arms state officials with strong enforcement tools to ensure compliance with the law. Consumers' personal information will be better protected.

In closing, I want to thank you for the opportunity to speak before you today in support of the Data Security and Breach Notification Act of 2010. Consumers Union appreciates this committee's interest in addressing issues of data security and consumer privacy. We believe that the passage of this bill will give rise to responsible data security policies and will increase consumer confidence in the marketplace.