Consumers Union
Nonprofit Publisher of Consumer Reports

April 24, 2007

The Honorable Mark Pryor
Chair
Commerce Subcommittee on Consumer Affairs,
Insurance, and Automotive Safety
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Consumers Union, the nonprofit publisher of *Consumer Reports*, appreciates your sponsorship of legislation addressing data privacy and security. Consumers are rightfully concerned about the privacy and security of sensitive personal information about them which is held by third parties. We appreciate your leadership in addressing this important matter.

In the past two years, security breaches have been announced involving over 150 million records containing sensitive personal information about individuals. At the same time, identity theft continues to bring U.S. consumers missed credit opportunities as well as lost time and added stress as the individual consumer must work to resolve the problems created by false accounts and unauthorized charges.

According to the Federal Trade Commission, there are an estimated 10 million U.S. identity theft victims each year. Based on this number, Consumers Union estimates that there are 19 new U.S. identity theft victims every minute. When new accounts are being opened using sensitive personal information, consumers spend an average of 77 hours to resolve the resulting problems, according to a 2007 Javelin Research study. Overall, according to a 2003 report to the FTC, U.S. consumers spend 297 million hours annually resolving the problems created by identity theft.

S. 1178, the Identity Theft Prevention Act, addresses these unpleasant facts of financial life. The legislation imposes an obligation on those who hold sensitive data to safeguard that data, requires notice to the consumer when safeguards have failed, and gives all consumers a tool to use proactively to prevent the new account form of identity theft. While Consumers Union supports many of the bill's provisions, we believe that the notice of security breach portion of the measure requires improvement because it excuses notice in some circumstances where consumers are currently receiving notice under strong state laws.

We appreciate that S. 1178 covers all types of security breaches, not only breaches of computerized information. This is very helpful, since paper records can contain the same type of sensitive personal information as computer records. However, this measure conditions, or "triggers" the obligation to give notice of a security breach on whether the breached entity "determines that the breach of security creates a reasonable risk of identity theft." While some

Consumers Union
Headquarters Office
101 Truman Avenue
Yonkers, New York 10703-1057
(914) 378-2029
(914) 378-2992 (fax)

Washington Office
1101 17th Street, NW #500
Washington, DC 20036
(202) 462-6262
(202) 265-9548 (fax)

West Coast Office
1535 Mission Street
San Francisco, CA 94103-2512
(415) 461-6747
(415) 431-0906 (fax)

South West Office
506 West 14th Street, Suite A
Austin, TX 78701
(512) 477-4431
(512) 477-8934 (fax)

state laws contain such a trigger, many do not. States such as California, New York, Illinois and Texas already require notice of breach without any risk standard, and we believe that national companies are giving notice to the higher standard of these existing state laws when they have customers located both inside and outside of these states whose records are part of the same breach.

We are deeply concerned that tying notice to an affirmative determination of risk will excuse notice in that most common of circumstances where there is simply not enough information to determine the level or nature of the risk due to incomplete information. For this reason, Consumers Union supports notice of breach requirements without triggers, loopholes or exceptions.

As a final note, we wish to express our support for your inclusion of a security freeze for all consumers. A security freeze is a powerful preventative tool for individuals. It enables consumers to take a step that will stop the opening of new accounts which require a credit check unless the consumer has expressly authorized the checking of the consumer's credit report or credit score by the entity considering opening a new account.

A security freeze lets a consumer stop thieves from opening false new credit accounts and other false accounts for which a credit review is part of the account opening process. A security freeze locks, or freezes, access to the consumer credit report and credit score, with appropriate limited exceptions. Without a credit report or credit score a business will not open a new account for a thief. As of April 20, 2007, 31 states plus the District of Columbia have enacted security freeze laws. The best of these state laws provide low fees, easy placement and lifting of the freeze and a method for consumers to get a temporary lift of the freeze within 15 minutes when the consumer wants to use his or her own credit.

The Identity Theft Prevention Act has many of the best features from state law, and permits state laws that are more protective of consumers to continue to operate. Adding freeze rights to federal law will not only serve the rest of the U.S., it also will heighten consumer awareness nationwide of this new self-help method for the prevention of new account identity theft, so that each U.S. consumer can make an individual choice about using this protection against new account ID theft.

We look forward to working with you to strengthen the notice of breach provisions of the Identity Theft Prevention Act and to enact strong data privacy legislation in the 110th Congress.

Sincerely,

Gail Hillebrand
Financial Services Campaign Leader
West Coast Office

cc: Senator John Sununu