Mrs. FEINSTEIN. Mr. President, I rise to introduce the Notification of Risk to Personal Data Act of 2003. This legislation will require that individuals are notified when their most sensitive personal information is stolen from a corporate or government database.

Specifically, the bill would require government or private entities to notify individuals if a data breach has compromised their Social Security number, driver's license number, credit card number, debit card number, or financial account numbers.

In most cases, if authorities know that someone is a victim of a crime, the victim is notified. But that isn't the case if an individual's most sensitive personal information is stolen from an electronic database.

Unfortunately, data breaches are becoming all too common. Consider the following incidents which have compromised the records of hundreds of thousands of Americans.

On April 5, 2002, a hacker broke into the electronic records of Steven P. Teale Data Center, the payroll facility for California State employees. The hacker compromises files containing the first initials, middle initials, and last names, Social Security numbers, and payroll deduction information of approximately 265,000 people. Despite the breathtaking potential harm of the crime, the breach was not publicly acknowledged and State employees were not made aware of their vulnerability to identify theft until May 24, 2002--17 days later.

On December 14, 2002, TriWest Health Care Alliance, a company that provides health care coverage for military personnel and their families, was burglarized at its Phoenix, AZ offices. Thieves broke into a management suite and stole laptop computers and computer hard drives containing the names, addressed, telephone numbers, birth dates and Social Security numbers of 562,000 military service members, dependents and retirees, as well as medical claims records for people on active duty in the Persian Gulf.

In February 2003, a hacker gained access to 10 million Visa, MasterCard, American Express Card and Discovery Card numbers from the databases of a credit processor, DPI Merchant services of Omaha, NE. Company officials maintained that the intruder did not obtain any personal information for these card numbers such as the account holder's name, address, telephone number or Social Security number. However, at least one bank canceled and replaced 8,800 cards when it found out about the security breach.

And in March of this year, a University of Texas student was charged with hacking into the university's computer system and stealing 55,000 Social Security numbers.

These are just some examples of the types of breaches that are occurring today. Except for California, which as a notification law going into effect in July, no State of Federal law requires companies or agencies to tell individuals of the misappropriation of their personal data.

I strongly believe Americans should be notified if a hacker gets access to their most personal data. This is both a matter of principle and a practical measure to curb identity theft.

Let me take a moment to describe the proposed legislation.

The Notification of Risk to Personal Data Act will set a national standard for notification of consumers when a data breach occurs.

Specifically, the legislation requires a business or government entity to notify an individual when there is a reasonable basis to conclude that a hacker or other criminal has obtained unencrypted personal data maintained by the entity.

Personal data is defined by the bill as an individual's Social Security number, State identification number, driver's license number, financial account number, or credit card number.

The legislation's notification scheme minimizes the burdens on companies or agencies that must report a data breach.

In general, notice would have to be provided to each person whose data was compromised in writing or through e-mail. But there are important exceptions.

First, companies that have developed their own reasonable notification policies are given a safe harbor under the bill and are exempted from its notification requirements.

Second, encrypted data is exempted.

Third, where it is too expensive or impractical, e.g., contact address information is incomplete, to notify every individual who is harmed, the bill allows entities to

send out an alternative form of notice called ``substitute notice." Substitute notice includes posting notice on a website or notifying major media.

Substitute notice would be triggered if any of the following factors exist: 1. the agency or person demonstrates that the cost of providing direct notice would exceed $250,000; 2. the affected class of subject persons to be notified exceeds 500,000; or 3. the agency or person does not have sufficient contact information to notify people whose information is at risk.

The bill has a tough, but fair enforcement regime. Entities that fail to comply with the bill will be subject to fines by the Federal Trade Commission of $5,000 per violation or up to $25,000 per day while the violation persists. State Attorneys General can also file suit to enforce the statute.

Additionally, the bill would allow California's new law to remain in effect, but preempt conflicting State laws. It is my understanding that legislators in a number of States are developing bills modeled after the California law. Reportedly, some of these bills have requirements that are inconsistent with the California legislation. It is not fair to put companies in a situation that forces them to comply with database notification laws of 50 different States.

I strongly believe individuals have a right to be notified when their most sensitive information is compromised--because it is truly their information. Ask the ordinary person on the street if he or she would like to know if a criminal had illegally gained access to their personal information from a database--the answer will be a resounding yes.

Enabling consumers to be notified in a timely manner of security breaches involving their personal data will help combat the growth scourge of identity theft. According to the Identity Theft Resources Center, a typical identity theft victim takes six to 12 months to discover that a fraud has been perpetuated against them.

As Linda Foley, Executive Director of the Identity Theft Resources center puts it: ``Identity theft is a crime of opportunity and time is essential at every junction. Every minute that passes after the breach until detection and notification increases the damage done to the consumer victim, the commercial entities, and law enforcement's ability to track and catch the criminals. It takes less than a minute to fill out a credit application and to start an action that could permanently affect the victim's life. Multiply that times hundreds of minutes, hundreds of opportunities to use or sell the information stolen and you just begin to understand the enormity of the problem that the lack of notification can cause."

If individuals are informed of the theft of their Social Security numbers or other sensitive information, they can take immediate preventative action.

They can place a fraud alert on their credit report to prevent crooks from obtaining credit cards in their name; they can monitor their credit reports to see if unauthorized activity has occurred; they can cancel any affected financial or consumer or utility accounts; they can change their phone numbers if necessary.

I look forward to working with my colleagues to pass this vitally needed legislation. This bill will give ordinary Americans more control and confidence about the safety of their personal information. Americans will have the security of knowing that should a breach occur, they will be notified and be able to take protective action.

I ask unanimous consent that the text of the bill be printed in the **RECORD**.