



## Senator Feinstein Continues Effort to Protect Individuals From Identity Theft

January 10, 2007

**Washington, DC** – U.S. Senator Dianne Feinstein (D-Calif.) today reintroduced two bills aimed at protecting individuals from identity theft by requiring businesses to notify consumers in the event of a security breach and prohibiting the sale or display of an individual's Social Security number without his or her consent.

Senator Feinstein said that the increased frequency of data breaches demonstrates that the legislation is needed sooner rather than later. Major data breaches have occurred in recent months at Boeing, UCLA, the Colorado Department of Human Services, Starbucks, the Chicago Voters' Database, and Akron Children's Hospital.

**"It's critical that victims of a security breach are informed promptly when their personal or financial information has been compromised,"** Senator Feinstein said. **"Individuals cannot take the appropriate steps to protect themselves if they are not armed with detailed information about the breach. Without that knowledge, individuals are left defenseless to identity thieves."**

**"If a person's social security number is compromised, the path to identity theft is a short one,"** Senator Feinstein said. **"Thieves can obtain social security numbers through public records – marriage licenses, professional licenses, and countless other public documents – many of which are available online. We must ensure that government agencies and businesses take responsibility and protect Americans' Social Security numbers."**

As Chairman of the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, Senator Feinstein intends to hold a hearing on the legislation and examine additional options for strengthening protections against identity theft early in the 110<sup>th</sup> Congress.

### **The Notification of Risk to Personal Data Act would:**

- Require a federal agency or business entity to notify an individual of a security breach involving personal data without unreasonable delay;
- Allow limited exemptions for law enforcement and national security reasons;

- Require media notice as well as individual notice;
  - Notice must include description of the type of personal data breached and a toll-free number to call for more information;
  - If more than 1,000 individuals must be notified, then the company or agency must coordinate with credit reporting agencies;
- Require notice to the Secret Service if records of more than 10,000 individuals are obtained or if the database breached contains more than one million entries, is owned by the federal government, or involves national security or law enforcement;
- Authorize the U.S. Attorney General and state Attorneys General to bring civil actions;
- Supersede any conflicting federal or state laws; and
- Authorize necessary appropriations.

**Social Security Number Misuse Prevention Act would:**

- Prohibit the sale or display of an individual's Social Security number to the general public without the individual's consent;
- Prohibit federal, state and local government agencies from displaying Social Security numbers on public records posted on the Internet or issued to the general public through CD-ROMs or other electronic media, or from printing them on government checks;
- Prevent the employment of inmates for tasks that would give them access to the Social Security numbers of other individuals;
- Provide some limitations on when a business can ask a customer for his or her Social Security number;
- Require a study of the current uses of Social Security numbers and the impact on privacy and data security; and
- Include both criminal and civil penalties.

In the 109<sup>th</sup> Congress, Senator Feinstein's data breach notification measure was included as part of a comprehensive data privacy bill that passed the Judiciary Committee on November 17, 2005, but did not get Senate floor action.

###