



Senate Judiciary Committee Approves Bill to Protect Americans from Identity Theft

-- Includes provision ensuring that individuals be notified following a database breach --
November 17, 2005

Washington, DC – The Senate Judiciary Committee today approved comprehensive data privacy bill that helps protect Americans from the growing epidemic of identity theft.

The bill is sponsored by Senators Arlen Specter (R-PA), Patrick Leahy (D-VT), Dianne Feinstein (D-Calif.), and Russell Feingold (D-WI). It would:

- Require that individuals be notified in the event of a data breach;
- Increase penalties for identity theft crimes;
- Regulate data brokers;
- Require security programs be implemented to protect personal data; and
- Require the federal government to evaluate the privacy and security systems of contractors.

“This is a bill whose time has come,” Senator Feinstein said. **“It is a very good bill. It strikes a good balance. I have been working on data privacy and security issues since the mid-1990s, and with every passing year, the need for such legislation has become all the more apparent. Americans deserve to be safe from identity theft. ”**

Earlier this year, Senator Feinstein introduced legislation that would require businesses or government agencies to notify individuals if a database has been broken into and personal data has been compromised, including Social Security numbers, driver's licenses and credit cards. Many of these provisions were incorporated into the larger data security bill.

“Over the past two years, there have been 35 major breaches, exposing more than 58 million people to identity theft,” **Senator Feinstein said.** “This bill will give all Americans the same rights that Californians have – to be notified when their personal data has been jeopardized and they are at risk of identity theft.”

Following is a summary of the key provisions of the bill:

NOTIFICATION – A federal agency or business entity must notify an individual of a security breach involving personal data without unreasonable delay following the discovery of the breach

and any measures necessary to assess the security breach and prevent further disclosures. Notice may be delayed or exempted for law enforcement and national security reasons. Notice must be provided in writing, by telephone, or by email. Notices given must include a description of the personal data breached and a toll-free number to call for more information and the toll free numbers of the major credit reporting agencies. Failure to provide notice will result in monetary penalties of \$1,000/day/individual with a maximum of \$1 million/violation.

INCREASED PENALTIES FOR IDENTITY THEFT CRIMES – Amends RICO to address the emergence of criminal organizations trafficking in large amounts of personal data to ensure that such criminal activity is covered under the law. Makes it a crime to intentionally and willfully conceal a data security breach. And, directs the U.S. Sentencing Commission to review and amend where necessary the federal sentencing guidelines to ensure they appropriately reflect the severity of the unauthorized or fraudulent use of personal data.

REGULATION OF DATA BROKERS – Requires data brokers disclose, for a reasonable fee (\$8 - \$12), personal data relating to an individual that is maintained by them for disclosure to third parties. The disclosure must include instructions on how individuals can correct inaccurate public and non-public record data. Failure of data brokers to do so will result in monetary penalties (\$1,000/day/violation up to \$250,000/violation).

DATA PRIVACY AND SECURITY PROGRAMS – Requires business entities with personal data records on more than 10,000 individuals to establish a data privacy and security program that includes risk management, employee training, vulnerability testing, security upgrades and scrutiny of service providers hired to process data. Financial institutions and HIPAA regulated entities already subject to similar requirements are exempt from the requirements of this Act. Failure to have appropriate data privacy and security programs under this Act will result in monetary penalties of \$5,000/day/violation with a maximum of \$500,000/violation.

SAFE HARBOR – Exempts entities from notifying individuals if they conduct a “risk assessment” which concludes that there is no “significant risk” that the security breach has resulted in, or will result in, harm to the individuals whose personal data was breached. This assessment will have to be provided to the U.S. Secret Service who can decide, after review of the reasons for claiming the safe harbor exemption, that notice is still required. Also, exempts business from notice if they have a program in place to prevent unauthorized financial transactions before they are charged to an individual’s account (i.e., credit/debit card fraud) and there is no other risk of harm to the individual.

GOVERNMENT CONTRACTORS – Requires the General Services Administration (GSA) to take data security practices into account when considering contract awards greater than \$500,000 and to include monetary penalties in such contracts for failure to comply with the data security requirements imposed under this Act. Requires the federal government to conduct audits of the data security practices of contractors and prohibits government agencies from entering into contracts with data brokers without first conducting a privacy impact assessment regarding the personal data they will be receiving and how safe and accurate it is.

ENFORCEMENT – The Federal Trade Commission and State attorneys general. In addition, the federal Attorney General can also bring civil actions against entities that fail to provide notice to individuals in the event of a data breach.

PREEMPTION – Subject matter pre-emption throughout the Act. The notification section also pre-empts all federal law as they relate to notice to individuals in the event of a data breach.

PERSONAL DATA – Is defined as non-truncated social security numbers, driver’s license numbers, passport numbers or alien registration numbers. In addition, “sensitive personally identifiable information” includes in certain circumstances home addresses or telephone numbers, mother’s maiden names and birthdates. It also includes biometric data and certain account information.

TYPES OF DATA – Only electronic data is covered under this Act, regardless of whether it is encrypted or not.

PRIVATE CAUSE OF ACTION – Not allowed under the Act.

SECURITY BREACH – Defined as a “compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization.”

DATA BROKER – Defined as a business entity which for monetary fees or dues regularly engages in the practice of “collecting, transmitting, or providing access” to personal data on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for purposes of providing that data to nonaffiliated third parties.

###