



Senator Feinstein Gains Republican Support for Identity Theft Notification Bill

-- Senator Kyl announces he will cosponsor Feinstein bill --
June 23, 2005

Washington, DC – The effort to pass legislation sponsored by Senator Dianne Feinstein (D-Calif.) requiring that individuals be notified when their personal data has been compromised and they are at risk for identity theft received a major boost today when Senator Jon Kyl (R-AZ) announced that he would cosponsor a modified version of Feinstein’s notification bill.

In the past two years, there have been 35 major database breaches, exposing more than 58 million Americans to identity theft.

“Day after day we hear about new data breaches, each one worse than the last,” Senator Feinstein said. **“This week, for instance, we heard about a breach which puts 40 million Americans at risk for identity theft. It is just the latest in a wave of incidents exposing nearly 58 million Americans.”**

“Today, only Californians and residents of a few other states have the right to be notified when their data has been compromised. Residents of New Hampshire, Vermont, and Mississippi deserve the same rights that Californians have. So let me offer my deepest thanks to Senator Kyl for cosponsoring this legislation. It is my hope that with his support we can move this bill out of the Judiciary Committee soon, and bring it to the Senate floor for a vote.”

“With the realities of identity theft a growing concern, this bill will give consumers the notification they need to protect themselves from potential misuse of their sensitive information,” Senator Kyl said.

Senator Kyl is the chairman of the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security. Senator Feinstein is the ranking member of that subcommittee.

The modified version of the bill includes the following provisions:

- **Notification** – Requires that the federal government and businesses notify individuals when there has been a data security breach which has resulted in, or in which there is a significant risk that it will result in harm to individuals.

- **Exceptions** – There are only two exceptions to immediate notification – for law enforcement or national security purposes.
- **Data Covered** – An individual's name in combination with their: Social Security number; driver's license or state issued identification number; Financial account /credit card/debit card number with any required password or code; Health information; or any other information regarding an individual deemed appropriate by the Federal Trade Commission.
- **Type of Data** – All data (encrypted, unencrypted, electronic and non-electronic data).
- **Trigger** – Notification is required when there is an unauthorized acquisition of personal information which compromises the security, confidentiality, or integrity of personal information in a manner that has resulted in, or there is a significant risk that it will result in, harm to the individual to whom the information relates.
- **Timeliness** – A government agency or a business 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.
- **Methods of Notification** – Notice must be provided to individuals either in writing or by e-mail. However, e-mail notice is only appropriate where an individual has previously consented to that agency or business to receive e-mail notices.
- **Alternative Notification** – Allows the government or businesses to maintain their own notification procedures by which they will send out timely notice according to the Act, if those procedures are part of an information security policy for the treatment of personal information.
- **Content of the Notice** – All notices must include: (1) a description of the type of personal data which has been, or could have been, compromised; (2) a toll-free telephone number for individuals to call to learn what type of personal data has been, or could have been, compromised and whether or not that individual's data may be at risk; and (3) toll-free telephone numbers and addresses for the major credit reporting agencies.
- **Fraud Alerts** – Affected individuals will be allowed to have an extended fraud alert of seven years placed on their credit reports. This is an expansion of current law in this area under the Fair Credit Reporting Act.
- **Penalties and Civil Remedies** – When a government agency or business fails to notify individuals of a breach of security involving their personal data in a timely manner, they will be subject to fines of not more than \$1,000 per individual whose personal data was, or is reasonably believed to have been, compromised OR not more than \$50,000 per day while the failure to notify persists. Injunctive relief is also available.

In addition, State Attorneys General (or any other State or local law enforcement agency authorized by the State Attorney General) may bring a civil action against a business in federal or state court to enjoin them from violating, or to enforce, the notification requirements of this bill. Civil actions can also be brought to obtain damages, restitution, or other monetary compensation on behalf of the residents of a State.

- **Enforcement** – The authority to enforce the notice requirements (including the assessment of fines) of this Act rests with the Federal Trade Commission, unless enforcement would be specifically committed by law or regulation to some other appropriate regulator.
- **Preemption** – The bill would preempt state laws as they relate to notification.
- **Effective Date** – The provisions of this bill will take effect six months after the date of enactment.

The legislation is also sponsored by Senator Mark Dayton (D-MN).

###