



E-Loan and ING Direct Endorse Feinstein Identity Theft Legislation  
-- *First Two Major Companies to Endorse Feinstein Bill* --  
June 7, 2005

**Washington, DC** – E-Loan and ING Direct today announced their support for legislation sponsored by U.S. Senator Dianne Feinstein (D-Calif.) that would require companies to notify individuals if their personal information has been compromised.

**“Identity theft is a vast and growing crime that affects nearly 10 million Americans each year,”** Senator Feinstein said. **“This problem is compounded by database breaches that expose thousands of individuals to identity theft in a single incident. So far this year there have been 11 database or security breaches where the personal information of nearly 8 million people was compromised. I welcome the support of E-LOAN and ING DIRECT for legislation I introduced to help protect consumers when they are unknowingly put at risk for identity theft.”**

**“In spite of the need for stronger privacy and identity theft legislation, many leading banks continue to argue that existing regulations are ‘adequate’ at providing the necessary level of protection to safeguard consumers’ personal financial data,”** said Chris Larsen, Chairman and Founder of E-LOAN. **“It is unfortunate that they’re choosing to take the short term view of maintaining the status quo rather than supporting legislation that helps to protect consumers and benefits everyone – including the financial industry – in the long run. We firmly support Senator Feinstein in her efforts to enact this legislation and applaud her for continuing this fight on behalf of all consumers.”**

**“ING DIRECT believes that each individual American has the right to control his or her personal information,”** said Arkadi Kuhlmann, President and CEO, ING DIRECT. **“This includes the right to know when the security of a company to which you have entrusted your most private information has been compromised. We support Senator Feinstein’s legislation and her efforts to address this widespread and devastating problem. We are urging Congress to seriously consider this bill.”**

Many incidents involving information scammed or stolen from large databases have been reported in the news recently, the most widely-known of which is ChoicePoint, a large data broker that sold personal information from 145,000 Americans to an identity theft ring posing as a legitimate business in September 2004. On April 13 the Senate Judiciary Committee held a hearing on this issue and Senator Feinstein’s bill.

Identity theft costs more than \$50 billion annually in the United States. The Federal Trade Commission (FTC) reports that California has the third-highest rate of identity theft per capita in the nation.

**Bill Summary**

The Notification of Risk to Personal Data Act (S. 751) requires a business or government entity to notify an individual in writing or email when it is believed that personal information – such as a Social Security number, driver’s license or state identification number, or credit card or bank account information – has been compromised.

There are only two exceptions where notification is not required: First, upon the written request of law enforcement for purposes of a criminal investigation; and second, for national security purposes.

In cases where written or e-mail notice is not possible due to the cost or number of individuals to be notified, substitute notice is acceptable. However, in order to qualify for substitute notice, the government or business must demonstrate that the cost of providing direct notice would exceed \$500,000 or 500,000 individuals to be notified. Substitute notice allows for notice to be done by an internet website posting or media release. Written or e-mail notice can also be substituted if the government agency or business does not have sufficient contact information to properly notify individuals.

The bill is based on the ground-breaking California law is the first and only State law requiring notification of individuals. But in fact, the legislation is stronger than the California law:

- It covers both electronic and non-electronic data – as well as encrypted and non-encrypted data. The California law only includes unencrypted, electronic data.
- It allows individuals to put a 7-year fraud alert on their credit report. The California law doesn’t address fraud alerts.
- It doesn’t include a major loophole allowing companies to follow weaker notification requirements – as the California law does.
- It lays out specific requirements for what must be included in notices, including:
  - a description of the data that may have been compromised;
  - a toll-free free number to learn what information and which individuals have been put at risk;
  - and the numbers and addresses for the three major credit reporting agencies.
- By contrast, California law is silent on what should be in notices.
- It has tougher civil penalties -- \$1,000 per individual they failed to notify or not more than \$50,000 per day while the failure to notify continues or existed. In California, a victim may bring a civil action to recover damages or the company may be enjoined from further violations.
- And it sets a national standard – so that individuals in Iowa, Oklahoma, and Maine have the same protections as consumers in California.
- The law would be enforced by the Federal Trade Commission or other relevant regulator, or by a State attorney general who could file a civil suit.

## Summary of Recent Database and Security Breaches

- **Citigroup** – personal information on 3.9 million consumer lending customers was lost by UPS while in transit to a credit bureau in June 2005.
- **Stanford University** – information including Social Security numbers on 9,600 clients of its Career Development Center, as well as on 300 recruiters, was exposed to hackers in May 2005.
- **Time Warner Inc.** – 40 computer backup tapes containing the names and social security numbers of more than 600,000 current and former employees and their dependents were lost by an outside storage company in May 2005.
- **UC San Francisco** – a computer unprotected by any firewalls or encryptions that stored the Social Security Numbers of 7,000 students, faculty, and staff was hacked in April 2005.
- **UC Berkeley** – a laptop was stolen from an unlocked office in March 2005. It contained the Social Security Numbers and other identifying information of 98,000 students, alumni, and applicants.  
**Also at UC Berkeley** – a database containing the Social Security Numbers and dates of birth of 600,000 students, faculty and alumni was hacked in October 2004.
- **Boston College** – 120,000 alumni's addresses and Social Security Numbers were compromised by hackers in March 2005.
- **DSW Shoe Warehouse** – hackers compromised customer databases in 103 shoe stores, gaining access to the credit cards of 1.5 million people in March 2005.
- **LexisNexis** – Identity thieves used stolen passwords to access the Social Security Numbers, driver's licenses and consolidated public records of 310,000 Americans in March 2005.
- **Bank of America** – backup computer tapes containing the records of over 1.2 million people disappeared in February 2005. Those affected included U.S. Senators and Representatives.
- **SAIC** – (a government security contractor) Laptops containing the Social Security numbers and other private information of 45,000 employees were stolen during a break-in in February 2005.
- **George Mason University** – 30,000 photographs and Social Security Numbers were compromised by hackers in January 2005.
- **ChoicePoint** – (a large data broker) sold personal information from 145,000 Americans to an identity theft ring posing as a legitimate business in September 2004. ChoicePoint had a similar breach in 2002, involving about 7,000 records.

- **HSBC Credit Cards** – Criminals may have obtained access to the credit card information in March 2004 of at least 180,000 people who used General Motors branded MasterCard to make purchases at Polo Ralph Lauren.
- **Data Processors International** – a database of 8 million credit card records was breached by hackers in February 2004.

###